IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor	: **Masaaki TAKASE, et al.**
Filed	: **Concurrently herewith**
For	: **COMMON KEY ENCRYPTION.....**
Serial No.	: **Concurrently herewith**

November 25, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRIORITY CLAIM AND

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2002-348748** filed **November 29, 2002,** a certified copy of which is enclosed.

Respectfully submitted,

Thomas J. Bean
Reg. No. 44,528

Katten Muchin Zavis Rosenman
575 Madison Avenue
New York, NY 10022-2585
(212) 940-8800
Docket No.: FUJY 20.758

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１１月２９日

出願番号
Application Number: 特願２００２－３４８７４８

[ST. 10/C]: [ＪＰ２００２－３４８７４８]

出願人
Applicant(s): 富士通株式会社

２００３年 ８月 ４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０６２２８１

【書類名】　特許願

【整理番号】　0253262

【提出日】　平成14年11月29日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/16

【発明の名称】　共通鍵暗号化通信システム

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号富士通株式会社内

【氏名】　高瀬　正明

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号富士通株式会社内

【氏名】　掛水　光明

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号富士通株式会社内

【氏名】　五十嵐　洋一郎

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号富士通株式会社内

【氏名】　谷口　浩之

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　山村　新也

【発明者】
【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号富士通西日本コミュニケーション・システムズ株式会社内
【氏名】　岩本　勝徳
【発明者】
【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号富士通西日本コミュニケーション・システムズ株式会社内
【氏名】　小金丸　啓
【発明者】
【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号富士通西日本コミュニケーション・システムズ株式会社内
【氏名】　若目田　宏
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【弁理士】
【氏名又は名称】　松倉　秀実
【連絡先】　０３－３６６９－６５７１
【手数料の表示】
【予納台帳番号】　012092
【納付金額】　21,000円
【その他】　国等の委託研究の成果に係る特許出願（平成１４年度通信・放送機構「ヒューマンセントリック　ユビキタスネ

ットワーク基盤システムに関する研究開発」委託研究、
産業活力再生特別措置法第３０条の適用を受けるもの）

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705606

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　共通鍵暗号化通信システム

【特許請求の範囲】

【請求項１】　鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、

前記鍵送信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第１保持手段と、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第１設定手段と、

を備え、

前記鍵受信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第２保持手段と、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第２設定手段と、

を備える、共通鍵暗号化通信システム。

【請求項２】　前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、

前記第１保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、

前記第１設定手段は、前記第１保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、請求項１に記載の共通鍵暗号化通信システム。

【請求項３】　前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、

前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する、請求項２に記載の共通鍵暗号化通信システム。

【請求項４】　前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第１送信手段をさらに備える、請求項２に記載の共通鍵暗号化通信システム。

【請求項５】　前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第２受信手段をさらに備え、

前記第２受信手段が暗号化鍵を受信した場合、

前記第２保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第２受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、

前記第２設定手段は、前記第２保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、請求項４に記載の共通鍵暗号化通信システム。

【請求項６】　前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第２送信手段を備え、

前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第１受信手段を備える、請求項１に記載の共通鍵暗号化システム。

【請求項７】　前記第１及び第２保持手段は、それぞれ初期化鍵を保持する、請求項４に記載の共通鍵暗号化通信システム。

【請求項８】　鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。

【請求項９】　鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の

暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。

【請求項１０】　鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、

前記鍵送信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、

送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、

前記鍵受信装置は、

前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、

送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は共通鍵を用いた暗号化方式を用いる場合の共通鍵の共有方法に関する。

【０００２】

【従来の技術】

ネットワークの発展に伴い、ネットワーク上を流れるトラフィックも多様化している。この中には他人に知られてはならない秘密情報等も含まれており、それを秘匿する手段としてIPsec等による暗号化通信技術が確立されている。

【０００３】

暗号化通信方式である VPN（Virtual Private Network）特に、IPsec（IP security protocol）を利用した通信方式では、暗号化通信の開始前に通信対象の端末が相互に IKE（Internet Key Exchange）プロトコルを利用して暗号鍵を交換し、通信時にこれを用いてデータの暗号/復号化を行うことが規定されている。

【０００４】

上述の暗号鍵は、同一の鍵内容を長時間利用すると悪意ある傍受者に鍵内容を解読される恐れがあることから、個々の鍵には有効期限が設定されており、この

期限を越えて通信に利用することができない規定となっている。このため、IPsecによるVPN通信中の端末は、当該有効期限の満了前に再度鍵交換手順を実施して新規に暗号鍵を取得して定期的に更新することで、暗号通信の堅牢性を確保している。

【０００５】

上述の一連の鍵交換機構では、各端末（通信のエンドポイント）が保持する暗号鍵は、現在通信中のものが満了する前に、次の鍵交換を実施し、この鍵交換が完了した時点で新たな鍵に切り替えて暗号化通信を継続することが可能である。

【０００６】

上述の機構は一対一の通信においては問題がないと考えられるが、一サーバに対し多数のクライアントが暗号化通信を行う場合には、サーバの鍵交換による負荷が問題になると考えられる。これを解決するためには例えばサーバからクライアントに鍵を配布する方法が考えられるが、この方法において定期的に鍵を更新する場合、鍵配布中や鍵を配布するためのメッセージが破棄された場合に通信が途切れてしまうという問題があった。即ち、鍵配布時の鍵紛失時のリカバリー手順は考慮されておらずVPNをモバイル通信と併用する際の懸念事項となる。

【０００７】

なお、インターネット等の標準的なプロトコルを利用しつつ、１つのセッション中における暗号化鍵の交換を可能として、通信データの機密性・秘蔵性を確保するものが知られている（例えば、特許文献１参照）。

【０００８】

【特許文献１】

特開２００２－２１７８９６号公報

【０００９】

【発明が解決しようとする課題】

本発明の課題は、共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続するための技術を提供することにある。

【００１０】

【課題を解決するための手段】

本発明は、上記課題を解決するために、鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第１保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第１設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第２保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第２設定手段と、を備える構成とした。

【００１１】

本発明によれば、鍵送信装置と鍵受信装置がそれぞれ、共通鍵として最新の暗号化鍵及び一世代前の二世代の暗号化鍵を保持するため、鍵送信装置が鍵受信装置に暗号化鍵等を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続することが可能となる。なお、鍵送信装置としては、Ｍｏｂｉｌｅ　ＩＰでのＨＡに限られない。例えば、インターネット上のサーバ等の情報処理端末であってもよい。また、鍵受信装置としては、Ｍｏｂｉｌｅ　ＩＰでのＭＮに限られない。例えば、インターネット上のサーバ等と通信可能な情報処理端末であってもよい。

【００１２】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、前記第１保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第１設定手段は、前記第１保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する。

【００１３】

このようにすれば、鍵送信装置において暗号化鍵を更新することが可能となる。

【００１４】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する。

【００１５】

このようにすれば、鍵送信装置は、自ら生成した鍵を取得することが可能となる。また、鍵送信装置は、外部の鍵生成部に鍵の生成を依頼してこの鍵を取得するようにしてもよいし、又は、自己又は外部が保持する鍵データベース等から鍵を読み出すようにしてもよい。

【００１６】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第１送信手段をさらに備える。この送信のタイミングとしては各種のものが考えられる。例えば、鍵受信装置から所定メッセージを受信した場合に送信するようにしてもよいし、自己でタイマを保持しておき、所定タイミングで送信するようにしてもよい。

【００１７】

このようにすれば、一（鍵送信装置）対多（鍵受信装置）の共通鍵暗号化通信における、鍵の共有に要する負荷が低減される。

【００１８】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第２受信手段をさらに備え、前記第２受信手段が暗号化鍵を受信した場合、前記第２保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第２受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第２設定手段は、前記第２保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する。

【００１９】

このようにすれば、鍵受信装置において暗号化鍵を更新することが可能となる。

【００２０】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第２送信手段を備え、前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第１受信手段を備える。

【００２１】

このようにすれば、鍵送信装置は、所定メッセージの受信をきっかけとして、鍵の生成や鍵の配布等を行うことが可能となる。

【００２２】

上記共通鍵暗号化通信システムにおいては、例えば、前記第１及び第２保持手段は、それぞれ初期化鍵を保持する。

【００２３】

このようにすれば、鍵受信装置の起動時（二世代の鍵のいずれも設定されていない状態）や、鍵受信装置からの鍵更新要求に対する鍵送信装置からの応答が得られない場合（鍵送信装置の障害等により鍵送信装置の二世代鍵が失われていると考えられる状態）であっても、その初期化鍵による暗号化が可能となるため、暗号化通信を継続することが可能となる。

【００２４】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵初期化要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵初期化要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第１保持手段は、共通の初期化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する。

【００２５】

このようにすれば、鍵送信装置は、鍵受信装置からの初期化要求メッセージに応じて、自己の暗号化鍵を初期化することが可能となる。

【００２６】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵更新要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵更新要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第１保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する。

【００２７】

このようにすれば、鍵送信装置は、鍵受信装置からの鍵更新要求メッセージに応じて、自己の暗号化鍵を更新することが可能となる。

【００２８】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、鍵更新時期を決定するための手段を備え、前記第２送信手段は、鍵更新時期に達した場合に、鍵更新要求メッセージを鍵送信装置に対して送信する。

【００２９】

このようにすれば、鍵受信装置は、所定タイミングで（例えば周期的に）、鍵更新要求メッセージを送信することが可能となる。

【００３０】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵送信装置は、鍵更新時期を決定するための手段を備え、第１送信手段は、鍵更新時期に達した場合に、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する。

【００３１】

このようにすれば、鍵送信装置は、鍵受信装置からの要求にかかわらず、自己の判断で、暗号化鍵を送信することが可能となる。

【００３２】

上記共通鍵暗号化通信システムにおいては、例えば、前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵再送要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵再送要求メッセージを受信した場合、第１送信手段は、前記取得手段によって取得した暗号化鍵

を鍵受信装置に対して送信する。

【００３３】

このようにすれば、鍵送信装置は、鍵受信装置からの鍵再送要求メッセージに応じて、暗号化鍵を送信することが可能となる。

【００３４】

上記共通鍵暗号化通信システムにおいては、例えば、前記第１送信手段は、前記第１及び第２保持手段がいずれの鍵も保持していない状態で、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する。この場合、初期化鍵を用いて通信することになる。

【００３５】

本発明は、鍵送信装置として次のように特定できる。鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。

【００３６】

なお、鍵送信装置としては、Ｍｏｂｉｌｅ　ＩＰでのＨＡに限られない。例えば、インターネット上のサーバ等の情報処理端末であってもよい。

【００３７】

また、本発明は、鍵受信装置として次のように特定できる。鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。

【００３８】

なお、鍵受信装置としては、Ｍｏｂｉｌｅ　ＩＰでのＭＮに限られない。例えば、インターネット上のサーバ等と通信可能な情報処理端末であってもよい。

【００３９】

また、本発明は、方法の発明として次のように特定できる。鍵送信装置と鍵受

信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。

【００４０】

【発明の実施の形態】

以下、本発明の実施の形態である共通鍵暗号化通信システムについて図面を参照しながら説明する。図１は、共通鍵暗号化通信システムの概略構成を説明するための図である。

【００４１】

図１に示すように、共通鍵暗号化通信システムは、鍵送信装置と鍵受信装置とを備えており、両者間で、所定タイミングで更新される共通鍵による暗号化通信を行う。鍵の配布は鍵送信装置が行う。このため、一（鍵送信装置）対多（鍵受信装置）の共通鍵暗号化通信における、鍵の共有に要する負荷が低減される。

【００４２】

従来、鍵送信装置と鍵受信装置がそれぞれ受信鍵を一つだけを管理していたので、鍵送信側が鍵を生成して自らに設定した後、生成した鍵を含む鍵配布メッセージを鍵受信側が受信して設定するまでの間、鍵の不一致のため暗号化通信が不可能になる。これを解決するため、本実施形態の共通鍵暗号化通信システムでは、双方が受信用に鍵を二世代保持、管理し（Ｎ番目の鍵及びＮ－１番目の鍵）、鍵送信側の暗号化鍵(送信用)には一世代前の鍵（Ｎ－１番目の鍵）を設定し（用い）、鍵受信側の暗号化鍵(送信用)には最新の鍵（Ｎ番目の鍵）を設定する（用いる）。また、双方とも復号化鍵(受信用)として最新/一世代前（Ｎ番目の鍵及びＮ－１番目の鍵）の双方を設定し、どちらでも復号できるようにする。

【００４３】

本実施形態においては、鍵送信装置と鍵受信装置との間でＭｏｂｉｌｅ　ＩＰ

ｖ６による通信を行うものとする。

【００４４】

まず、Ｍｏｂｉｌｅ　ＩＰｖ６の概要について説明する。Ｍｏｂｉｌｅ　ＩＰｖ６は、移動端末としてのＭＮ(mobile node)が当初のネットワーク・セグメント（ホームネットワークという）とは異なるネットワーク・セグメントへ移動しても、同一のＩＰアドレスで通信を継続するための仕組みを提供する。そのために、当初のネットワーク・セグメントにルーター等のＨＡ(home agent)が設けられている。

【００４５】

ＭＮは、当初のネットワーク・セグメントとは異なるネットワーク・セグメントへ移動したことを検出すると、その移動先ネットワーク上のアドレス（一時的なcare-ofアドレス。気付アドレスともいう）を生成してＨＡに登録する。具体的には、ＭＮは、登録要求(ＢＵ:Binding Update)をＨＡに対して送信する。これにより、新しいcare-ofアドレス（送信元アドレスとして含まれている）をＨＡに知らせる。

【００４６】

ＨＡは、ＭＮからの登録要求（ＢＵ）を受信すると、care-ofアドレスを登録する。これとともに、ＨＡは、登録応答(ＢＡ:binding acknowledgement)をその登録要求送信元のＭＮに対して送信する。以後、ＨＡは、登録されているＭＮ宛のパケットを受け取った場合には、そのパケットをカプセル化し（care-ofアドレスが宛先アドレス）トンネリングにより移動先のネットワーク・セグメントへ転送する。これにより、ＭＮは当初のネットワーク・セグメントとは異なるネットワーク・セグメントへ移動しても、同一のＩＰアドレスで通信を継続することが可能となっている。

【００４７】

次に、鍵送信装置及び鍵受信装置の構成について図面を参照しながら説明する。本実施形態においては、上記ＨＡ(home agent)が鍵送信装置１００に、ＭＮ(mobile node)が鍵受信装置２００に、それぞれ相当する。図２は、鍵送信装置（ＨＡ）の構成例を説明するための図である。図３は、鍵受信装置（ＭＮ）の構成

例を説明するための図である。

【００４８】

図２に示すように、鍵送信側装置（ＨＡ）１００は、パケット送受信部１０１、鍵生成／管理部１０２、暗号化／復号化部１０３、及び、プロトコル制御部１０４等を備えている。また、ＳＰＩ値を用いて鍵の更新/鍵の初期化を判断する場合は、ＳＰＩ-鍵対応テーブルを鍵生成/管理部が保持する(図２１参照)。

【００４９】

パケット送受信部１０１は、Ｍｏｂｉｌｅ　ＩＰｖ６のネットワークに接続されており、鍵受信装置（ＭＮ）２００等からの自己宛のパケット（例えば、所定メッセージを含むパケット）を受信したり、鍵受信装置（ＭＮ）２００等宛のパケットをネットワークへ送出する。このパケット送受信部１０１により、鍵受信装置（ＭＮ）２００からの所定メッセージ（鍵初期化要求メッセージ、鍵更新要求メッセージ、又は、鍵再送要求メッセージ等）を受信できるため、鍵受信装置（ＭＮ）２００からの要求により、強制的に鍵更新を行うことが可能となる。また、更新した鍵を鍵受信装置（ＭＮ）２００へ送信することが可能となる。

【００５０】

鍵生成／管理部１０２は、所定タイミングで暗号化鍵を生成（又は、外部の鍵生成部に暗号化鍵の生成を依頼してこれを取得、又は、自己又は外部が保持する鍵データベース等から暗号化鍵を読み出し）する。鍵生成／管理部１０２は、その生成等された暗号化鍵（最新の暗号化鍵）とその直前のタイミングで生成等された暗号化鍵（一世代前の暗号化鍵）、及び、予め設定されている初期化用鍵を保持、管理する。

【００５１】

これらの鍵は後述のように更新されるが、その場合でも、鍵生成／管理部１０２は、その更新（生成等）された暗号化鍵（最新の暗号化鍵）とその直前のタイミングで更新（生成等）された暗号化鍵（一世代前の暗号化鍵）、及び、予め設定（又は配布）されている初期化用鍵を保持、管理する。この鍵生成／管理部１０２により、一定周期又は鍵受信装置（ＭＮ）２００から要求があった場合に動的に鍵を生成し、更新することが可能になる。

【００５２】

また、この鍵生成／管理部１０２が受信用の鍵を二世代管理することにより、鍵受信装置（ＭＮ）２００が一世代前の鍵又は最新の鍵のどちらでパケットを暗号化しても、復号化することが可能となる。また、この鍵生成／管理部１０２が送信用の鍵を一つ管理、設定することにより、鍵送信装置（ＨＡ）１００は、一世代前の鍵でパケットを暗号化し、送信することが可能となる。

【００５３】

また、この鍵生成／管理部１０２が初期化用の鍵を一つ管理、設定することにより、この鍵で暗号化された動的鍵初期化要求メッセージを復号化することができる。また、この鍵で暗号化されたことを鍵送信装置（ＨＡ）１００が認識することにより、動的鍵の初期化を行うことが可能となる。

【００５４】

以下、Ｎ回目の鍵の作成で作られた鍵をＮ番目の鍵と呼ぶ。即ち、初回の鍵配布で鍵送信装置（ＨＡ）１００から鍵受信装置（ＭＮ）２００へ送信される鍵は、１番目の鍵である。鍵生成／管理部１０２は、鍵受信装置（ＭＮ）２００ごと（ＭＮが複数の場合）に二世代の鍵及び初期化用鍵を保持、管理する。鍵生成／管理部１０２は、通常、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する。

【００５５】

暗号化／復号化部１０３は、鍵受信装置（ＭＮ）２００からの受信パケットが暗号化されている場合に、その受信パケットを受信用の暗号化鍵（のいずれか）で復号化したり、鍵受信装置（ＭＮ）２００に対する送信パケットを送信用の暗号化鍵で暗号化するためのものである。暗号化／復号化部１０３は、その復号化又は暗号化の際には、鍵生成／鍵管理部１０２を参照して、適切な暗号化鍵を使用する。

【００５６】

プロトコル制御部１０４は、暗号化／復号化部１０３により復号化された鍵受信装置（ＭＮ）２００からの受信パケットの内容を判定したり、鍵受信装置（ＭＮ）２００に対して送信する鍵配布メッセージを作成したりするためのものであ

る。

【００５７】

図３に示すように、鍵受信装置（ＭＮ）２００は、パケット送受信部２０１、鍵管理部２０２、暗号化／復号化部２０３、及び、プロトコル制御部２０４等を備えている。

【００５８】

パケット送受信部２０１は、Ｍｏｂｉｌｅ　ＩＰｖ６のネットワークに接続されており、鍵送信装置（ＨＡ）１００等からの自己宛のパケットを受信したり、鍵送信装置（ＨＡ）１００等宛のパケットをネットワークへ送出する。このパケット送受信部２０１が鍵配布メッセージを受信することにより、鍵送信装置（ＨＡ）１００からの鍵の配布が可能となる。

【００５９】

鍵管理部２０２は、鍵送信装置（ＨＡ）１００から配布される鍵配布メッセージに含まれる暗号化鍵（最新の鍵及び一世代前の暗号化鍵）、及び、予め設定されている初期化用鍵（いずれの鍵も鍵送信装置（ＨＡ）１００と共通）を保持、管理する。

【００６０】

鍵管理部２０２は、通常、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する。これらの鍵は後述のように更新されるが、その場合でも、鍵管理部２０２は、その更新（生成等）された暗号化鍵（最新の暗号化鍵）とその直前のタイミングで更新（生成等）された暗号化鍵（一世代前の暗号化鍵）、及び、予め設定（又は配布）されている初期化用鍵を保持、管理する。

【００６１】

この鍵管理部２０２が受信用の鍵を二世代管理／設定することにより、鍵送信装置（ＨＡ）１００が最新鍵又は一世代前の鍵のどちらでパケットを暗号化しても、復号化することが可能となる。また、この鍵管理部２０２が送信用の鍵を一つ管理／設定することにより、鍵受信装置（ＭＮ）２００は最新の鍵でパケットを暗号化し、送信することが可能となる。

【００６２】

また、この鍵生成／管理部１０２が初期化用の鍵を一つ管理／設定することにより、動的鍵初期化要求メッセージも暗号化することができ、またこの鍵で暗号化されたことを鍵送信側装置が認識することによって初期化を行うことが可能となる。

【００６３】

暗号化／復号化部２０３は、鍵送信装置（ＨＡ）１００からの受信パケットが暗号化されている場合に、その受信パケットを受信用の暗号化鍵（のいずれか）で復号化したり、鍵送信装置（ＨＡ）１００に対する送信パケットを送信用の暗号化鍵で暗号化するためのものである。暗号化／復号化部２０３は、その復号化又は暗号化の際には、鍵管理部２０２を参照して、適切な暗号化鍵を使用する。

【００６４】

プロトコル制御部２０４は、暗号化／復号化部２０３により復号化された鍵送信装置（ＨＡ）１００からの所定メッセージ（鍵初期化メッセージ、鍵更新メッセージ、鍵再送要求メッセージ等）を作成したりするためのものである。このプロトコル制御部２０４が鍵更新要求メッセージ又はこれに相当するメッセージを生成することにより、鍵受信側装置（ＭＮ）２００の意向又は鍵配布メッセージがネットワーク上で破棄された場合に、鍵受信装置（ＭＮ）２００が最新の鍵を要求することが可能になる。また、プロトコル制御部２０４が鍵初期化要求メッセージ又はこれに相当するメッセージを生成することにより、鍵受信装置（ＭＮ）２００障害等で双方の鍵の初期化が必要となった場合に、鍵送信側装置にそれを要求することが可能となる。

【００６５】

次に、上記構成の共通鍵暗号化通信システムにおける暗号化通信の動作について図面を参照しながら説明する。

【００６６】

まず、鍵受信装置（ＭＮ）２００からの所定メッセージにより、鍵送信装置（ＨＡ）１００が暗号化鍵を更新、鍵受信装置（ＭＮ）２００に対して配布する処理について説明する。ここでは、鍵受信装置（ＭＮ）２００からの登録要求（Ｂ

Ｕ）とともに所定メッセージを送信し、鍵送信装置（ＨＡ）１００からの登録応答（ＢＡ）ともに鍵配布メッセージを送信するものとする。

【００６７】

（１）鍵受信装置（ＭＮ）２００からの所定メッセージが鍵初期化メッセージである場合の動作例（その１）

【００６８】

図４は、鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図５及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図６は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１７は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。図１８は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。

【００６９】

ここでは、鍵受信装置（ＭＮ）２００起動時には鍵受信装置（ＭＮ）２００及び鍵送信装置（ＨＡ）１００共に動的鍵（Ｎ番目の鍵、Ｎ－１番目の鍵）は保持（設定）されておらず、初期化鍵のみが双方に保持（設定）されているものとする。

【００７０】

鍵受信装置（ＭＮ）２００は起動すると初期設定を行う。ここでは、暗号化鍵(送信用)及び復号化鍵(受信用)として共に初期化鍵が設定される。次に、図４、図５に示すように、鍵受信装置（ＭＮ）２００は、鍵を初期化すべき事象が発生したとして（Ｓ１００）、鍵初期化要求メッセージを含むＢＵを作成する。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部２０４は、拡張ヘッダ部分（又はペイロード部分）に鍵初期化要求メッセージ及びＢＵを設定（又は配置）したＩＰパケットを作成する（Ｓ１０１）。

【００７１】

このＢＵ（ＩＰパケット）は後述のように暗号化／復号化部２０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＨＡ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部２０４は、そのＢＵ（

ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【００７２】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、プロトコル制御部２０４は、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＢＵ（ＩＰパケット）は送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部２０４は、作成したＢＵ（ＩＰパケット）を暗号化／復号化部２０３へ渡す（Ｓ１０２）。

【００７３】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ１０３）（送信用の鍵(初期化鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ１０４）。暗号化／復号化部２０３による暗号化は次のようにして行う。例えば、鍵初期化要求メッセージ及びＢＵがＩＰｖ６のＩＰパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部２０３は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する（トンネル・モード）。一方、鍵初期化要求メッセージ及びＢＵがＩＰパケットのペイロードに配置されている場合には、暗号化／復号化部２０３は、ＩＰヘッダ以外のデータ部を暗号化する（トランスポート・モード）。又は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ１０５）。

【００７４】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ１０６）。

【００７５】

図６、図１７に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を受信する（Ｓ１０７）。パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３へ渡す（Ｓ１０８）。暗号化／復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成／管理部１０２を参照し、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ１０９）、登録要求（ＢＵ）の処理後、プロトコル制御部１０４へ渡す（Ｓ１１０）。

【００７６】

プロトコル制御部１０４は、暗号化／復号化部１０３からのパケットの内容を判定し（Ｓ１１１）、鍵初期化要求メッセージであればそれを鍵生成／管理部１０２に通知する（Ｓ１１２）。

【００７７】

鍵生成／管理部１０２は、新たな鍵を生成する（Ｓ１１３）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を初期化する（Ｓ１１４）。

【００７８】

具体的には、暗号化鍵(送信用)として初期化鍵を、 復号化鍵(受信用)として新たな鍵及び初期化鍵を、それぞれ設定する（図１参照）。そして、鍵生成／管理部１０２は、その鍵の設定後、その生成した新たな鍵をプロトコル制御部１０４に渡す（Ｓ１１５）。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

【００７９】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ１１６）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰ

パケット）を作成する。

【００８０】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【００８１】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＢＡ（ＩＰパケット）は送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ１１７）。

【００８２】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ１１８）（送信用の鍵（初期化鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ１１９）。暗号化／復号化部による暗号化は次のようにして行う。例えば、鍵配布メッセージ及びＢＡがＩＰｖ６のＩＰパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する（トンネル・モード）。

【００８３】

一方、鍵配布メッセージ及びＢＡがＩＰパケットのペイロードに配置されている場合には、暗号化／復号化部は、ＩＰヘッダ以外のデータ部を暗号化する（トランスポート・モード）。又は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する。暗号化／復号化部は、暗号化したＢＡ（ＩＰパケット）をパケット送受信部１０１へ渡す（Ｓ１２０）。

【００８４】

パケット送受信部１０１は、暗号化／復号化部１０３からのＢＡ（ＩＰパケット）を鍵受信装置（ＭＮ）２００に対して送信する（Ｓ１２１）。

【００８５】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（ＩＰパケット）を受信する（Ｓ１２２）。パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【００８６】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たな鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【００８７】

鍵管理部２０２は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

【００８８】

（２）鍵受信装置（ＭＮ）２００からの所定メッセージが鍵初期化メッセージである場合の動作例（その２）

【００８９】

図４は、鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図５及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図６は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１７は、鍵送信装置（ＨＡ）における概略処理を説明するためのフロー

チャートである。図１８は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。

【００９０】

ここでは、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００それぞれは、最新の鍵（Ｎ番目の鍵）及び一世代前の鍵（Ｎ－１番目の鍵）を保持、管理している（図１参照）。そして、鍵送信装置（ＨＡ）１００の暗号化鍵(送信用)として一世代前の鍵（Ｎ－１番目の鍵）が、鍵受信装置（ＭＮ）の暗号化鍵(送信用)として最新の鍵（Ｎ番目の鍵）が、それぞれ使用可能であるように設定されている。また、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００双方の復号化鍵(受信用)として、最新の鍵（Ｎ番目の鍵）、一世代前の鍵（Ｎ－１番目の鍵）の二つが使用可能であるように設定されている(図1参照)。

【００９１】

鍵受信装置（ＭＮ）２００の要求による鍵の初期化には、鍵受信装置（ＭＮ）２００の再起動時等がある。図４、図５に示すように、鍵受信装置（ＭＮ）２００は、鍵受信装置（ＭＮ）２００内部で鍵の初期化を決定した場合（Ｓ１００）、鍵初期化要求メッセージを作成する。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部２０４は、拡張ヘッダ部分（又はペイロード部分）に鍵初期化要求メッセージ及びＢＵを設定（又は配置）したＩＰパケットを作成する（Ｓ１０１）。

【００９２】

このＢＵ（ＩＰパケット）は後述のように暗号化／復号化部２０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＨＡ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部２０４は、そのＢＵ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【００９３】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含ま

れるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ番目の鍵を指定するデータが設定される。プロトコル制御部２０４は、作成したＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を暗号化／復号化部２０３へ渡す（Ｓ１０２）。

【００９４】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ１０３）（送信用の鍵(Ｎ番目の鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ１０４）。この暗号化の方法についてはすでに述べた。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ１０５）。

【００９５】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ１０６）。

【００９６】

図６、図１７に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を受信し（Ｓ１０７）、鍵の生成と設定の初期化を行う。

【００９７】

具体的には、パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３に渡す（Ｓ１０８）。暗号化/復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成/管理部１０２を参照し、そのＳＰＩ値によって指定される鍵（ここではＮ番目の鍵）でパケットを復号し（Ｓ１０９）、登録要求（ＢＵ）の処理後、プロトコル制御部１０４に渡す（Ｓ１１０）。

【００９８】

プロトコル制御部１０４は、暗号化／復号化部１０３からのパケットの内容を判定し（Ｓ１１１）、鍵初期化要求メッセージであればそれを鍵生成/管理部１

０２に通知する（Ｓ１１２）。

【００９９】

鍵生成/管理部１０２は、新たな鍵（Ｎ＋１番目の鍵）を生成する（Ｓ１１３）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を初期化する（Ｓ１１４）。具体的には、鍵生成／管理部１０２は、復号化鍵(受信用)として新たにＮ＋１番目の鍵と初期化鍵を設定し、Ｎ－１番目の鍵を削除する。

【０１００】

また、鍵生成／管理部１０２は、暗号化鍵(送信用)として新たに初期化鍵を設定し、Ｎ－１番目の鍵を削除する。なお、初期化鍵をＮ－１番目の鍵として扱い、次回の鍵更新時には初期化鍵を削除する。そして、鍵生成/管理部１０２は、鍵の設定を更新後、その作成した新たな鍵（Ｎ＋１番目の鍵）をプロトコル制御部１０４に渡す（Ｓ１１５）。

【０１０１】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ１１６）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０１０２】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので

、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

【０１０３】

ここでは、後述のようにＩＰパケットは送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ１１７）。

【０１０４】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ１１８）（送信用の鍵（初期化鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ１１９）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０３は、暗号化したＩＰパケットをパケット送受信部１０１へ渡す（Ｓ１２０）。

【０１０５】

パケット送受信部１０１は、暗号化／復号化部１０３からのＩＰパケットを鍵受信装置（ＭＮ）２００に対して送信する（Ｓ１２１）。

【０１０６】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【０１０７】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たなＮ＋１番目の鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０１０８】

鍵管理部２０２は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部２０２は、暗号化

鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。

【０１０９】

（３）鍵受信装置（ＭＮ）２００からの所定メッセージが鍵更新要求メッセージである場合の動作例

【０１１０】

図８は、鍵受信装置（ＭＮ）からの鍵更新要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図９及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図１０は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１７は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。図１８及び図２０は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。

【０１１１】

ここでは、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００それぞれは、最新の鍵（Ｎ番目の鍵）及び一世代前の鍵（Ｎ－１番目の鍵）を保持、管理している（図１参照）。そして、鍵送信装置（ＨＡ）１００の暗号化鍵(送信用)として一世代前の鍵（Ｎ－１番目の鍵）が、鍵受信装置（ＭＮ）の暗号化鍵(送信用)として最新の鍵（Ｎ番目の鍵）が、それぞれ使用可能であるように設定されている。

【０１１２】

また、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００双方の復号化鍵(受信用)として、最新の鍵（Ｎ番目の鍵）、一世代前の鍵（Ｎ－１番目の鍵）の二つが使用可能であるように設定されている(図1参照)。また、鍵送信装置（ＨＡ）１００でＮ＋１番目の鍵が生成され、その鍵が鍵受信装置（ＭＮ）２００に配布されるものとする(図８、図９参照)。

【０１１３】

本例では、鍵受信装置（ＭＮ）２００が鍵の更新を判断するため、鍵受信装置（ＭＮ）２００の鍵管理部２０１に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはＭｏｂｉｌｅ　ＩＰｖ６のＢＡメッセージと共に送信されるも

のとする。この鍵更新タイマにより、自らの鍵更新ポリシに従って、鍵更新要求メッセージを送信することが可能となる。

【０１１４】

図８、図９、図２０に示すように、鍵受信装置（ＭＮ）２００は、鍵受信装置（ＭＮ）２００内部で鍵の更新を決定した場合（Ｓ２００）（ここでは鍵管理部２０１において鍵更新タイマが満了した場合）、鍵更新要求メッセージを作成する。鍵管理部２０１において鍵更新タイマが満了すると、そのことをプロトコル制御部２０４に通知する（Ｓ２０１）。

【０１１５】

これによりプロトコル制御部２０４は、ＢＵ送信を検知する（Ｓ２０２）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部２０４は、拡張ヘッダ部分（又はペイロード部分）に鍵更新要求メッセージ及びＢＵを設定（又は配置）したＩＰパケットを作成する（Ｓ２０３）。

【０１１６】

このＢＵ（ＩＰパケット）は後述のように暗号化／復号化部２０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部２０４は、そのＢＵ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【０１１７】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ番目の鍵を指定するデータが設定される。プロトコル制御部２０４は、作成したＢＵ（鍵更新要求メッセージを含むＩＰパケット）を暗号化／復号化部２０３へ渡す（Ｓ２０４）。

【０１１８】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ２０５）（送信用の鍵(Ｎ番目の鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ２０６）。この暗号化の方法についてはすでに述べた。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ２０７）。

【０１１９】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ２０８）。

【０１２０】

図１０、図１７に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵更新要求メッセージを含むＩＰパケット）を受信し（Ｓ２０９）、鍵の生成と更新を行う。

【０１２１】

具体的には、パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３に渡す（Ｓ２１０）。暗号化/復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成/管理部１０２を参照し（Ｓ２１１）、そのＳＰＩ値によって指定される鍵（ここではＮ番目の鍵）でパケットを復号し（Ｓ２１２）、登録要求（ＢＵ）の処理後、プロトコル制御部１０４に渡す（Ｓ２１３）。

【０１２２】

プロトコル制御部１０４は、暗号化／復号化部１０３からのパケットの内容を判定し（Ｓ２１４）、鍵更新要求メッセージであればそれを鍵生成/管理部１０２に通知する（Ｓ２１５）。

【０１２３】

鍵生成/管理部１０２は、新たな鍵(Ｎ＋１番目の鍵)を生成する（Ｓ２１６）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定をする（Ｓ２１７）。具体的には、復号化鍵(受信用)として新たにＮ＋１番

目の鍵を設定し、Ｎ－１番目の鍵を削除する。また、暗号化鍵(送信用)として新たにN番目の鍵を設定し、Ｎ－１番目の鍵を削除する。そして、鍵生成／管理部１０２は、その鍵の設定を更新後、その生成した新たな鍵（Ｎ＋１番目の鍵）をプロトコル制御部１０４に渡す（Ｓ２１８）。

【０１２４】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ２１９）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０１２５】

このＩＰパケットは後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

【０１２６】

ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ－１番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ－１番目の鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ２２０）。

【０１２７】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ２２１）（送信用の鍵（Ｎ－１番目の鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ２２２）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０３は、暗号化したＩＰパケットをパケット送受信部１０１へ渡す（Ｓ２２３

）。

【０１２８】

パケット送受信部１０１は、暗号化／復号化部１０３からのＩＰパケット（鍵配布メッセージを含むＩＰパケット）を鍵受信装置（ＭＮ）に対して送信する（Ｓ２２４）。

【０１２９】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。鍵受信装置（ＭＮ）２００はそのＩＰパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２９）。

【０１３０】

具体的には、パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここではＮ－１番目の鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【０１３１】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たなＮ＋１番目の鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０１３２】

鍵管理部２０２は、復号化鍵（受信用）として新たにその抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部２０２は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

（４）鍵配布メッセージが破棄された場合のＭＮの動作例

【０１３３】

図１１は、鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図１２及び図７

は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図１３は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１７は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。図１８は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。

【０１３４】

ここでは、上記（３）鍵受信装置（ＭＮ）２００からの所定メッセージが鍵更新要求メッセージである場合の動作例において、鍵送信装置（ＨＡ）１００からの鍵配布メッセージ（Ｎ＋１番目の鍵を含む）を含むＢＡ（ＩＰパケット）が、鍵受信装置（ＭＮ）２００に到達せずに、途中で破棄されたものとする(図１１、図１２、図１３参照)。この場合、鍵送信側装置（ＨＡ）１００のみ動的に更新される鍵が更新された状態となる（図１６参照）。

【０１３５】

図１１、図１２に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００に対して送信したＢＵ（ＩＰパケット）に対するＢＡ（ＩＰパケット）を受信しないこと（例えばＢＵ送信後の一定期間内にＢＡを受信しないこと）を感知すると（Ｓ３００）、再送のためのＢＵ（鍵再送要求メッセージを含むＩＰパケット）を上記鍵更新要求メッセージ等と同様にプロトコル制御部２０４によって作成し（Ｓ３０１）、これを暗号化／復号化部２０３へ渡す（Ｓ３０２）。

【０１３６】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ３０３）（送信用の鍵(Ｎ番目の鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ３０４）。この暗号化の方法についてはすでに述べた。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ３０５）。

【０１３７】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ３０６）。

【０１３８】

図１３、図１７に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵再送要求メッセージを含むＩＰパケット）を受信し（Ｓ３０７）、鍵の再送を行う。

【０１３９】

具体的には、パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３に渡す（Ｓ３０８）。暗号化/復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成/管理部１０２を参照し（Ｓ３０９）、そのＳＰＩ値によって指定される鍵（ここではＮ番目の鍵）でパケットを復号し（Ｓ３１０）、登録要求（ＢＵ）の処理後、プロトコル制御部１０４に渡す（Ｓ３１１）。

【０１４０】

プロトコル制御部１０４は、暗号化／復号化部１０３からのパケットの内容を判定し（Ｓ３１２）、鍵再送要求メッセージであればそれを鍵生成/管理部１０２に通知する（Ｓ３１３）。

【０１４１】

鍵生成/管理部１０２は、新たな鍵を生成すること無く、前回配布して途中で破棄された最新の鍵(Ｎ＋１番目の鍵)をプロトコル制御部１０４に渡す（Ｓ３１４）。

【０１４２】

プロトコル制御部１０４は鍵配布メッセージを上記と同様に作成する（Ｓ３１５）。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ３１６）。

【０１４３】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ３１７）（送信用の鍵（Ｎ番目の鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ３１８）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０２は、暗号化したＢＡ（ＩＰパケット）をパケット送受信部１０１へ渡す（Ｓ３１９）。

【０１４４】

パケット送受信部１０１は、暗号化／復号化部からのＢＡ（ＩＰパケット）を鍵受信装置（ＭＮ）２００に対して送信する（Ｓ３２０）。

【０１４５】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。鍵受信装置（ＭＮ）２００は、上記と同様にそのＩＰパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２３～Ｓ１２９）。

以上述べたように、本動作例では、鍵送信側装置（ＨＡ）１００は一世代前の動的鍵を暗号化鍵（送信用）として使用することにより、動的鍵配布メッセージ（鍵配布メッセージともいう）が破棄されても通信が可能となる。

【０１４６】

（５）鍵送信側装置(ＨＡ)の障害時等の鍵初期化手順

【０１４７】

鍵送信装置（ＨＡ）１００の障害時等の鍵の初期化手順は以下である。ここでは、上記（３）鍵受信装置（ＭＮ）２００からの所定メッセージが鍵更新要求メッセージである場合の動作例において、鍵送信装置（ＨＡ）１００の障害等により鍵送信装置（ＨＡ）の動的に更新される鍵（Ｎ番目の鍵及びＮ－１番目の鍵）はすべて失われ、初期化用鍵のみが設定されているものとする。

【０１４８】

鍵受信装置（ＭＮ）１００は、鍵送信装置（ＨＡ）１００に対して送信したＢＵ（鍵更新要求メッセージを含むＩＰパケット）に対するＢＡ（ＩＰパケット）を一定期間後も受信しないことを検知すると、鍵送信装置（ＨＡ）１００の障害等が考えられるため、ＢＵ（鍵更新要求メッセージを含むＩＰパケット）を再送する。

【０１４９】

鍵受信装置（ＭＮ）２００は、その再送したＢＵ（ＩＰパケット）に対するＢＡを一定期間後も受信しないことを検知すると、動的に更新される鍵の設定を初期化し、鍵初期化要求メッセージを含むＢＵを図５に示すように生成して（Ｓ１

０１～Ｓ１０５）鍵送信装置（ＨＡ）１００に送信する（Ｓ１０６）。

【０１５０】

鍵送信装置（ＨＡ）１００は、図６及び図１７に示すように、鍵受信装置（ＭＮ）からのＢＵに鍵初期化要求が含まれることを検知すると（Ｓ１０７～Ｓ１１１）、上記と同様に、鍵初期化メッセージ受信時の処理を行い（Ｓ１１３～Ｓ１１５）、ＢＡに最新の鍵を含んだ鍵配布メッセージを付加し（Ｓ１１６）、鍵受信装置（ＭＮ）に送信する（Ｓ１１７～Ｓ１２１）。

【０１５１】

図７、図１８に示すように、鍵受信装置（ＭＮ）は、鍵配布メッセージが付加されたＢＡを受信すると（Ｓ１２２）、その中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２３～Ｓ１２９）。これについてはすでに述べたものと同様である。

【０１５２】

以上述べたように、本動作例によれば、鍵受信装置（ＭＮ）２００が鍵更新要求メッセージ又はそれに相当するメッセージを再送することにより、正常な状態（最新の鍵が鍵受信装置（ＭＮ）２００の送受信用に設定された状態）に復帰することが可能となる。また、鍵更新要求メッセージを再送してもその返答として鍵配布メッセージが鍵受信装置に届かない場合、鍵受信装置（ＭＮ）２００は鍵初期化要求メッセージを鍵送信装置（ＨＡ）１００に送信することによって、初期化を行う。

【０１５３】

以上述べたように、本動作例では、鍵受信側装置の障害等で鍵受信側装置と鍵送信側装置の動的鍵の不一致が起きた場合、動的鍵初期化メッセージ又はそれに相当するメッセージを鍵受信側装置が送信することにより、双方の動的鍵を初期化することが可能となる。

【０１５４】

（６）鍵送信側装置(ＨＡ)が鍵の更新を判断する場合のＨＡの動作例

【０１５５】

図１４は、鍵送信側装置(ＨＡ)が鍵の更新を判断して、動的鍵（共通鍵）を配

布する手順を説明するためのシーケンス図である。図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図１５は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１８は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。図１９は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【０１５６】

ここでは、鍵送信装置（ＨＡ）１００が鍵の更新（タイミング）を判断するため、鍵送信装置（ＨＡ）１００の鍵生成/管理部１０２に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはＭｏｂｉｌｅ　ＩＰｖ６のＢＡメッセージと共に送信されるものとする。この鍵更新タイマにより、一定周期で鍵の更新を行うことが可能となる。また、鍵送信装置（ＨＡ）１００はＮ－１番目の鍵とＮ番目の鍵を保持しているとし、鍵送信装置（ＨＡ）１００でＮ＋１番目の鍵が生成され、その鍵が鍵受信装置（ＭＮ）２００に配布されるものとする。

【０１５７】

図１４、図１５に示すように、鍵生成/管理部１０２において鍵送信装置（ＨＡ）１００の鍵更新タイマが満了すると（Ｓ４００）、そのことをプロトコル制御部１０４に通知し（Ｓ４０１）、プロトコル制御部１０４はそれを鍵受信装置（ＭＮ）２００ごとに保持する。例えば、プロトコル制御部１０４は、該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグをオンにセットする（Ｓ４１２）。

【０１５８】

鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（これには所定メッセージは含まれていない）を受信すると、ＢＵ処理を実行するとともに（Ｓ４０２）、プロトコル制御部１０４を参照して、そのＢＵ送信元の鍵受信装置（ＭＮ）２００の鍵更新タイマが満了したか否かを判定する。該当する鍵更新タイマが満了していれば（例えば該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグがオンにセットされていれば）、プロトコル制御部１０４は、ＢＡを作成する際、鍵生成／管理部１０２に鍵の更新を要求する。

【０１５９】

鍵生成/管理部１０２は、新たな鍵(Ｎ＋１番目の鍵)を生成する（Ｓ４０３）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこれを取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を更新する（Ｓ４０４）。具体的には、復号化鍵(受信用)として新たにＮ＋１番目の鍵を設定し、Ｎ－１番目の鍵を削除する。また、暗号化鍵(送信用)として新たにＮ番目の鍵を設定し、Ｎ－１番目の鍵を削除する。そして、鍵生成／管理部１０２は、その鍵の設定を更新後、その生成した新たな鍵（Ｎ＋１番目の鍵）をプロトコル制御部１０４に渡す（Ｓ４０５）。

【０１６０】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ４０６）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０１６１】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＭＮ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【０１６２】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ－１番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ－１番目の鍵を指定するデータが設定される。プロトコル制御部１０４は、作成し

たＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ４０７）。

【０１６３】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ４０８）（送信用の鍵（Ｎ－１番目の鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ４０９）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０３は、暗号化したＩＰパケットをパケット送受信部１０１へ渡す（Ｓ４１０）。

【０１６４】

パケット送受信部１０１は、暗号化／復号化部１０３からのＩＰパケット（鍵配布メッセージを含むＩＰパケット）を鍵受信装置（ＭＮ）に対して送信する（Ｓ４１１）。なお、ＢＡの送信が完了すると、該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグはオフにセットされる。

【０１６５】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。鍵受信装置（ＭＮ）２００はそのＩＰパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２９）。

【０１６６】

具体的には、パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここではＮ－１番目の鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【０１６７】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たなＮ＋１番目の鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０１６８】

鍵管理部２０２は、復号化鍵（受信用）として新たにその抽出した新たな鍵を

設定する（Ｓ１２９）。また、鍵管理部２０２は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

【０１６９】

次に、他の実施形態について説明する。

【０１７０】

ここでは、ＩＰｓｅｃによる暗号化通信を行っており、上記の実施形態とは異なり所定メッセージを用いることなく、そのＳＰＩ値により鍵の初期化/鍵の更新を判断する。鍵送信装置（ＨＡ）１００は、鍵－ＳＰＩ対応テーブル（図２１参照）を保持しており、鍵受信装置（ＭＮ）２００からのＢＵ（所定メッセージを含まないＩＰパケット）に含まれるＳＰＩ値とそのテーブルを照合することで、受信パケットがどの鍵で暗号化されたのかを判定する。他の構成については、上記実施形態と同様であるので、その説明は省略する。

【０１７１】

（７）鍵受信装置（ＭＮ）２００からのＢＵが初期化鍵で暗号化されている場合の動作例（その１）

【０１７２】

図２２は、鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図５及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図２３は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図２８は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【０１７３】

ここでは、鍵受信装置（ＭＮ）２００起動時には鍵受信装置（ＭＮ）２００及び鍵送信装置（ＨＡ）１００共に動的鍵（Ｎ番目の鍵、Ｎ－１番目の鍵）は保持（設定）されておらず、初期化鍵のみが双方に保持（設定）されているものとする。

【０１７４】

鍵受信装置（ＭＮ）２００は起動すると初期設定を行う。ここでは、暗号化鍵

(送信用)及び復号化鍵(受信用)として共に初期化鍵が設定される。次に、図２２、図５に示すように、鍵受信装置（ＭＮ）２００は、鍵を初期化すべき事象が発生したとして（Ｓ５００）、ＢＵを作成する。ここでは、上記実施形態と異なり、ＢＵに鍵初期化要求メッセージを含まない。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部２０４は、拡張ヘッダ部分（又はペイロード部分）にＢＵを設定（又は配置）したＩＰパケットを作成する（Ｓ５０１）。

【０１７５】

このＢＵ（ＩＰパケット）は後述のように暗号化／復号化部２０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＨＡ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部２０４は、そのＢＵ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【０１７６】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、プロトコル制御部２０４は、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＢＵ（ＩＰパケット）は送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部２０４は、作成したＢＵ（ＩＰパケット）を暗号化／復号化部２０３へ渡す（Ｓ５０２）。

【０１７７】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ５０３）（送信用の鍵(初期化鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ５０４）。暗号化／復号化部２０３による暗号化は次のようにして行う。

【０１７８】

例えば、鍵初期化要求メッセージ及びＢＵがＩＰｖ６のＩＰパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部２０３は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する（トンネル・モード）。一方、鍵初期化要求メッセージ及びＢＵがＩＰパケットのペイロードに配置されている場合には、暗号化／復号化部２０３は、ＩＰヘッダ以外のデータ部を暗号化する（トランスポート・モード）。

【０１７９】

又は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ５０５）。

【０１８０】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ５０６）。

【０１８１】

図２３、図２８に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を受信する（Ｓ５０７）と、その受信パケットからＳＰＩ値を抽出する（Ｓ５０８）。又は、暗号化／復号化部がこのＳＰＩ値を抽出するようにしてもよい。パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３へ渡す（Ｓ５０９）。

【０１８２】

暗号化／復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成／管理部１０２を参照し、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ５１０）、登録要求（ＢＵ）の処理後、その復号化したパケットとＳＰＩ値とをプロトコル制御部１０４へ渡す（Ｓ５１１）。

【０１８３】

プロトコル制御部１０４は、鍵生成／管理部１０２を参照して（Ｓ５１２）、鍵－ＳＰＩ値テーブルと抽出したＳＰＩ値とを照合することで、暗号化／復号化部１０３からのパケットがどの鍵で暗号化されているかを判定（Ｓ５１３）する

。そして、プロトコル制御部１０４は、それが初期化鍵を用いて暗号化されたことを意味していると判定したのであれば、それを鍵生成／管理部１０２に通知する（Ｓ５１４）。

【０１８４】

鍵生成／管理部１０２は、新たな鍵を生成する（Ｓ５１５）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を初期化するとともに、鍵－ＳＰＩ対応テーブルを初期化する（Ｓ５１６、Ｓ５１７）。

【０１８５】

具体的には、暗号化鍵(送信用)として初期化鍵を、復号化鍵(受信用)として新たな鍵及び初期化鍵を、それぞれ設定する（図１参照）。そして、鍵生成／管理部１０２は、その鍵の設定後、その生成した新たな鍵をプロトコル制御部１０４に渡す（Ｓ５１８）。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

【０１８６】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ５１９）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０１８７】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので

、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

【０１８８】

ここでは、後述のようにＢＡ（ＩＰパケット）は送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ５２０）。

【０１８９】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ５２１）（送信用の鍵（初期化鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ５２２）。暗号化／復号化部による暗号化は次のようにして行う。例えば、鍵配布メッセージ及びＢＡがＩＰｖ６のＩＰパケットの拡張ヘッダに配置されている場合には、暗号化／復号化部は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する（トンネル・モード）。

【０１９０】

一方、鍵配布メッセージ及びＢＡがＩＰパケットのペイロードに配置されている場合には、暗号化／復号化部は、ＩＰヘッダ以外のデータ部を暗号化する（トランスポート・モード）。又は、ＩＰヘッダとデータ部をともに暗号化して、それに新たなＩＰヘッダを付加する。暗号化／復号化部は、暗号化したＢＡ（ＩＰパケット）をパケット送受信部１０１へ渡す（Ｓ５２３）。

【０１９１】

パケット送受信部１０１は、暗号化／復号化部１０３からのＢＡ（ＩＰパケット）を鍵受信装置（ＭＮ）２００に対して送信する（Ｓ５２４）。

【０１９２】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（ＩＰパケット）を受信する（Ｓ１２２）。パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０

４へ渡す（Ｓ１２６）。

【０１９３】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たな鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０１９４】

鍵管理部２０２は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。ここで、初期化鍵を一世代前の鍵として設定するようにすれば、二回目以降の動的鍵配布と同様な処理が可能となる。

【０１９５】

（８）鍵受信装置（ＭＮ）２００からのＢＵが鍵初期化鍵で暗号化されている場合の動作例（その２）

【０１９６】

図２２は、鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図５及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図２３は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図２８は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【０１９７】

ここでは、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００それぞれは、最新の鍵（Ｎ番目の鍵）及び一世代前の鍵（Ｎ－１番目の鍵）を保持、管理している（図１参照）。そして、鍵送信装置（ＨＡ）１００の暗号化鍵(送信用)として一世代前の鍵（Ｎ－１番目の鍵）が、鍵受信装置（ＭＮ）の暗号化鍵(送信用)として最新の鍵（Ｎ番目の鍵）が、それぞれ使用可能であるように設定されている。また、鍵送信装置（ＨＡ）１００、鍵受信装置（ＭＮ）２００双方の復号化鍵(受信用)として、最新の鍵（Ｎ番目の鍵）、一世代前の鍵（Ｎ－１番目の

鍵）の二つが使用可能であるように設定されている(図1参照)。

【０１９８】

鍵受信装置（ＭＮ）２００の要求による鍵の初期化には、鍵受信装置（ＭＮ）２００の再起動時等がある。図２２、図５に示すように、鍵受信装置（ＭＮ）２００は、鍵受信装置（ＭＮ）２００内部で鍵の初期化を決定した場合（Ｓ５００）、ＢＵを作成する。ここでは、上記実施形態と異なり、ＢＵに鍵初期化要求メッセージを含まない。本実施形態ではＭｏｂｉｌｅ．ＩＰｖ６を用いているので、例えば、プロトコル制御部２０４は、拡張ヘッダ部分（又はペイロード部分）にＢＵを設定（又は配置）したＩＰパケットを作成する（Ｓ５０１）。

【０１９９】

このＢＵ（ＩＰパケット）は後述のように暗号化／復号化部２０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＨＡ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部２０４は、そのＢＵ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。

【０２００】

ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ番目の鍵を指定するデータが設定される。プロトコル制御部２０４は、作成したＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を暗号化／復号化部２０３へ渡す（Ｓ５０２）。

【０２０１】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ５０３）（送信用の鍵(Ｎ番目の鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ５０４）。この暗号化の方法についてはすでに述べた。暗号

化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ５０５）。

【０２０２】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ５０６）。

【０２０３】

図２３、図２８に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（鍵初期化要求メッセージを含むＩＰパケット）を受信し（Ｓ５０７）と、その受信パケットからＳＰＩ値を抽出する（Ｓ５０８）。又は、暗号化／復号化部がこのＳＰＩ値を抽出するようにしてもよい。そして、鍵の生成と設定の初期化を行う。

【０２０４】

具体的には、パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３に渡す（Ｓ５０９）。暗号化/復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成/管理部１０２を参照し、そのＳＰＩ値によって指定される鍵（ここではN番目の鍵）でパケットを復号し（Ｓ５１０）、登録要求（ＢＵ）の処理後、その復号化したパケットとＳＰＩ値とをプロトコル制御部１０４に渡す（Ｓ５１１）。

【０２０５】

プロトコル制御部１０４は、鍵生成／管理部１０２を参照して（Ｓ５１２）、鍵－ＳＰＩ値テーブルと抽出したＳＰＩ値とを照合することで、暗号化／復号化部１０３からのパケットがどの鍵で暗号化されているかを判定する（Ｓ５１３）。そして、プロトコル制御部１０４は、それが初期化鍵を用いて暗号化されたことを意味していると判定したのであれば、それを鍵生成/管理部１０２に通知する（Ｓ５１４）。

【０２０６】

鍵生成/管理部１０２は、新たな鍵（Ｎ＋１番目の鍵）を生成する（Ｓ５１５）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこの鍵を含むメッセージとして取得する、又は、自己又は外部が

保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を初期化するとともに、鍵－ＳＰＩ対応テーブルを初期化する（Ｓ５１６、Ｓ５１７）。具体的には、鍵生成／管理部１０２は、復号化鍵(受信用)として新たにＮ＋１番目の鍵と初期化鍵を設定し、Ｎ－１番目の鍵を削除する。また、鍵生成／管理部１０２は、暗号化鍵(送信用)として新たに初期化鍵を設定し、Ｎ－１番目の鍵を削除する。なお、初期化鍵をＮ－１番目の鍵として扱い、次回の鍵更新時には初期化鍵を削除する。そして、鍵生成/管理部１０２は、鍵の設定を更新後、その作成した新たな鍵（Ｎ＋１番目の鍵）をプロトコル制御部１０４に渡す（Ｓ５１８）。

【０２０７】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ５１９）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０２０８】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

【０２０９】

ここでは、後述のようにＩＰパケットは送信用の鍵（初期化鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとして初期化鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ５２０）。

【０２１０】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ５２１）（送信用の鍵（初期化鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ５２２）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０３は、暗号化したＩＰパケットをパケット送受信部１０１へ渡す（Ｓ５２３）。

【０２１１】

パケット送受信部１０１は、暗号化／復号化部１０３からのＩＰパケットを鍵受信装置（ＭＮ）２００に対して送信する（Ｓ５２４）。

【０２１２】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここでは初期化鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【０２１３】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たなＮ＋１番目の鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０２１４】

鍵管理部２０２は、復号化鍵（受信用）として新たに（初期化鍵に加えて）その抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部２０２は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた初期化鍵を削除する（初期化鍵そのものは削除されない）。

【０２１５】

（９）鍵送信側装置(ＨＡ)が鍵の更新を判断する場合のＨＡの動作例

【０２１６】

図１４は、鍵送信側装置(ＨＡ)が鍵の更新を判断して、動的鍵（共通鍵）を配

布する手順を説明するためのシーケンス図である。図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図１５は、鍵送信装置（ＨＡ）に着目したシーケンス図である。図１８は、鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。図１９は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。図２８は、鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【０２１７】

ここでは、鍵送信装置（ＨＡ）１００が鍵の更新（タイミング）を判断するため、鍵送信装置（ＨＡ）１００の鍵生成/管理部１０２に鍵更新タイマが内蔵されているものとし、鍵配布メッセージはＭｏｂｉｌｅ　ＩＰｖ６のＢＡメッセージと共に送信されるものとする。この鍵更新タイマにより、一定周期で鍵の更新を行うことが可能となる。また、鍵送信装置（ＨＡ）１００はＮ－１番目の鍵とＮ番目の鍵を保持しているとし、鍵送信装置（ＨＡ）１００でＮ＋１番目の鍵が生成され、その鍵が鍵受信装置（ＭＮ）２００に配布されるものとする。

【０２１８】

図２４に示すように、鍵生成/管理部１０２において鍵受信装置（ＭＮ）１００の鍵更新タイマが満了すると（Ｓ６００）、そのことをプロトコル制御部１０４に通知し（Ｓ６０１）、プロトコル制御部１０４はそれを鍵受信装置（ＭＮ）２００ごとに保持する。例えば、プロトコル制御部１０４は、該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグをオンにセットする。

【０２１９】

鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（これには所定メッセージは含まれていない）を受信すると、ＢＵ処理を実行するとともに（Ｓ６０２）、その受信パケットからＳＰＩ値を抽出する（Ｓ６１３）。そして、暗号化／復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成／管理部１０２を参照し、そのＳＰＩ値によって指定される鍵（ここではＮ番目の鍵）でパケットを復号する（Ｓ６１４）。

【０２２０】

プロトコル制御部１０４は、鍵生成／管理部１０２を参照して鍵－ＳＰＩ値テ

ーブルと抽出したＳＰＩ値とを照合することで、受信パケットがどの鍵で暗号化されているかを判定する（Ｓ６１５）。そして、プロトコル制御部１０４は、それがN番目の鍵を用いて暗号化されたことを意味していると判定したのであれば（Ｓ６１６）、そのＢＵ送信元の鍵受信装置（ＭＮ）２００の鍵更新タイマが満了したか否かを判定する（Ｓ６１７）。

【０２２１】

該当する鍵更新タイマが満了していれば（Ｓ６１７：Ｙｅｓ）（例えば該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグがオンにセットされていれば）、プロトコル制御部１０４は、ＢＡを作成する際、鍵生成／管理部１０２に鍵の更新を要求する。

【０２２２】

鍵生成/管理部１０２は、新たな鍵(Ｎ＋１番目の鍵)を生成する（Ｓ６０３）（又は、何らかの手段で新たな鍵を取得する。例えば、外部の鍵生成部に鍵の生成を依頼してこれを取得する、又は、自己又は外部が保持する鍵データベース等から鍵を読み出す。）。鍵生成／管理部１０２は、鍵の設定を更新するとともに、鍵－ＳＰＩ対応テーブルを更新する（Ｓ６０４、Ｓ６０５）。

【０２２３】

具体的には、復号化鍵(受信用)として新たにＮ＋１番目の鍵を設定し、Ｎ－１番目の鍵を削除する。また、暗号化鍵(送信用)として新たにN番目の鍵を設定し、Ｎ－１番目の鍵を削除する。そして、鍵生成／管理部１０２は、その鍵の設定を更新後、その生成した新たな鍵（Ｎ＋１番目の鍵）をプロトコル制御部１０４に渡す（Ｓ６０６）。

【０２２４】

プロトコル制御部１０４は鍵配布メッセージを含む登録応答（ＢＡ）を作成する（Ｓ６０７）。本実施形態ではＭｏｂｉｌｅ　ＩＰｖ６を用いているので、例えば、プロトコル制御部１０４は、拡張ヘッダ部分（又はペイロード部分）に鍵配布メッセージ（新たな鍵を含む）及びＢＡを設定（又は配置）したＢＡ（ＩＰパケット）を作成する。

【０２２５】

このＢＡ（ＩＰパケット）は後述のように暗号化／復号化部１０３により暗号化されるので、その暗号化に用いた鍵を受信側（ＭＮ）で知ることができるように（即ち受信側で復号できるように）、プロトコル制御部１０４は、そのＢＡ（ＩＰパケット）にＡＨ(authentication header)又はＥＳＰ(encapsulating security payload)を適用する。なお、ＡＨのみを適用した場合は、ＢＡに含んで配布する鍵を別途暗号化（ＡＨで用いる鍵を流用することも可能）する必要がある。ＡＨ又はＥＳＰにはＳＰＩ(security parameters index)のフィールドが含まれるので、このフィールドにその暗号化に用いた鍵を指定するためのデータを設定する。

【０２２６】

ここでは、後述のようにＩＰパケットは送信用の鍵（Ｎ－１番目の鍵）で暗号化されるため、その暗号化に用いた鍵を指定するためのデータとしてＮ－１番目の鍵を指定するデータが設定される。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ６０８）。

【０２２７】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ６０９）（送信用の鍵（Ｎ－１番目の鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ６１０）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０３は、暗号化したＩＰパケットをパケット送受信部１０１へ渡す（Ｓ６１１）。

【０２２８】

パケット送受信部１０１は、暗号化／復号化部１０３からのＩＰパケット（鍵配布メッセージを含むＩＰパケット）を鍵受信装置（ＭＮ）に対して送信する（Ｓ６１２）。なお、ＢＡの送信が完了すると、該当する鍵受信装置（ＭＮ）２００に対する鍵更新タイマ満了フラグはオフにセットされる。

【０２２９】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する（Ｓ１２２）。鍵受信装置（ＭＮ）２００はそのＩＰパケット中に含まれる鍵を

暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２９）。

【０２３０】

具体的には、パケット送受信部２０１は、受信したパケットが暗号化されていれば暗号化／復号化部２０３へ渡す（Ｓ１２３）。暗号化／復号化部２０３は、受信したパケットのＳＰＩ値及び鍵管理部２０２を参照し（Ｓ１２４）、そのＳＰＩ値によって指定される鍵（ここではＮ－１番目の鍵）でパケットを復号化し（Ｓ１２５）、プロトコル制御部２０４へ渡す（Ｓ１２６）。

【０２３１】

プロトコル制御部２０４は暗号化／復号化部２０３からのパケットの内容を判定し（Ｓ１２７）、鍵配布メッセージであれば鍵（ＨＡで生成された新たなＮ＋１番目の鍵）を抽出し、その抽出した鍵を鍵管理部２０２に渡す（Ｓ１２８）。

【０２３２】

鍵管理部２０２は、復号化鍵（受信用）として新たにその抽出した新たな鍵を設定する（Ｓ１２９）。また、鍵管理部２０２は、暗号化鍵（送信用）として新たにその抽出した新たな鍵を設定し、送信用として設定されていた鍵を削除する。

【０２３３】

（１０）鍵配布メッセージが破棄された場合のＭＮの動作例

【０２３４】

図２５は、鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。図２６及び図７は、鍵受信装置（ＭＮ）に着目したシーケンス図である。図２７は、鍵送信装置（ＨＡ）に着目したシーケンス図である。

【０２３５】

ここでは、鍵送信装置（ＨＡ）１００からの鍵配布メッセージ（Ｎ＋１番目の鍵を含む）を含むＢＡ（ＩＰパケット）が、鍵受信装置（ＭＮ）２００に到達せずに、途中で破棄されたものとする(図２２、図２６参照)。この場合、鍵送信側装置（ＨＡ）１００のみ動的に更新される鍵が更新された状態となる（図１６参照）。図２８は、鍵送信装置（ＨＡ）における概略処理を説明するためのフロー

チャートである。

【０２３６】

図２５、図２６に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００に対して送信したＢＵ（ＩＰパケット）に対するＢＡ（ＩＰパケット）を受信しないこと（例えばＢＵ送信後の一定期間内にＢＡを受信しないこと）を感知すると（Ｓ７００）、再送のためのＢＵ（鍵再送要求メッセージを含むＩＰパケット）を上記鍵更新要求メッセージ等と同様にプロトコル制御部２０４によって作成し（Ｓ７０１）、これを暗号化／復号化部２０３へ渡す（Ｓ７０２）。

【０２３７】

暗号化／復号化部２０３は、鍵管理部２０２を参照して（Ｓ７０３）（送信用の鍵(Ｎ番目の鍵)を用いて）プロトコル制御部２０４からのＢＵ（ＩＰパケット）を暗号化する（Ｓ７０４）。この暗号化の方法についてはすでに述べた。暗号化／復号化部２０３は、暗号化したＢＵ（ＩＰパケット）をパケット送受信部２０１へ渡す（Ｓ７０５）。

【０２３８】

パケット送受信部２０１は、暗号化／復号化部２０３からのＢＵ（ＩＰパケット）を鍵送信装置（ＨＡ）１００に対して送信する（Ｓ７０６）。

【０２３９】

図２７に示すように、鍵送信装置（ＨＡ）１００は、鍵受信装置（ＭＮ）２００からのＢＵ（これには鍵再送要求メッセージを含まない）を受信すると（Ｓ７０７）、その受信パケットからＳＰＩ値を抽出する（Ｓ７０８）。又は、暗号化／復号化部がこのＳＰＩ値を抽出するようにしてもよい。

【０２４０】

具体的には、パケット送受信部１０１は、その受信したパケットが暗号化されていれば暗号化／復号化部１０３に渡す（Ｓ７０９）。暗号化/復号化部１０３は、受信したパケットのＳＰＩ値及び鍵生成/管理部１０２を参照し（Ｓ７１０）、そのＳＰＩ値によって指定される鍵（ここではＮ番目の鍵）でパケットを復号し（Ｓ７１１）、登録要求（ＢＵ）の処理後、その復号化したパケットとＳＰ

Ｉ値とをプロトコル制御部１０４に渡す（Ｓ７１２）。

【０２４１】

プロトコル制御部１０４は、鍵生成／管理部１０２を参照して（Ｓ７１３）、鍵－ＳＰＩ値テーブルと抽出したＳＰＩ値とを照合することで、暗号化／復号化部１０３からのパケットがどの鍵で暗号化されているかを判定する（Ｓ７１４）。そして、プロトコル制御部１０４は、それがＮ番目の鍵であれば、鍵受信装置（ＭＮ）２００がＮ＋１番目の鍵（最新の鍵）を受信していないと判断できるため（鍵再送要求メッセージ受信に相当する）、それを鍵生成/管理部１０２に通知する（Ｓ７１５）。

【０２４２】

鍵生成/管理部１０２は、新たな鍵を生成すること無く、前回配布して途中で破棄された最新の鍵(Ｎ＋１番目の鍵)をプロトコル制御部104に渡す（Ｓ７１６）。

【０２４３】

プロトコル制御部１０４は鍵配布メッセージを上記と同様に作成する（Ｓ７１７）。プロトコル制御部１０４は、作成したＢＡ（ＩＰパケット）を暗号化／復号化部１０３へ渡す（Ｓ７１８）。

【０２４４】

暗号化／復号化部１０３は、鍵生成／管理部１０２を参照して（Ｓ７１９）（送信用の鍵（Ｎ番目の鍵）を用いて）そのＢＡ（ＩＰパケット）を暗号化する（Ｓ７２０）。この暗号化の方法についてはすでに述べた。暗号化／復号化部１０２は、暗号化したＢＡ（ＩＰパケット）をパケット送受信部１０１へ渡す（Ｓ７２１）。

【０２４５】

パケット送受信部１０１は、暗号化／復号化部からのＢＡ（ＩＰパケット）を鍵受信装置（ＭＮ）２００に対して送信する（Ｓ７２２）。

【０２４６】

図７、図１８に示すように、鍵受信装置（ＭＮ）２００は、鍵送信装置（ＨＡ）１００からのＢＡ（鍵配布メッセージが付加されたＩＰパケット）を受信する

（Ｓ１２２）。鍵受信装置（ＭＮ）２００は、上記と同様にそのＩＰパケット中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２３～Ｓ１２９）。

以上述べたように、本動作例では、鍵送信側装置（ＨＡ）１００は一世代前の動的鍵を暗号化鍵（送信用）として使用することにより、動的鍵配布メッセージ（鍵配布メッセージともいう）が破棄されても通信が可能となる。

【０２４７】

（１１）鍵送信側装置(ＨＡ)の障害時等の鍵初期化手順

【０２４８】

鍵送信装置（ＨＡ）１００の障害時等の鍵の初期化手順は以下である。

【０２４９】

ここでは、鍵送信装置（ＨＡ）１００の障害等により鍵送信装置（ＨＡ）の動的に更新される鍵（Ｎ番目の鍵及びＮ－１番目の鍵）はすべて失われ、初期化用鍵のみが設定されているものとする。一方、鍵受信装置（ＭＮ）は動的に更新される鍵（Ｎ番目の鍵及びＮ－１番目の鍵）を保持しているものとする。

【０２５０】

鍵受信装置（ＭＮ）１００は、鍵送信装置（ＨＡ）１００に対して送信したＢＵ（鍵更新要求メッセージ等を含まない）に対するＢＡ（ＩＰパケット）を一定期間後も受信しないことを検知すると、鍵送信装置（ＨＡ）１００の障害等が考えられるため、ＢＵ（鍵更新要求メッセージを含まない）を再送する。

【０２５１】

鍵受信装置（ＭＮ）２００は、その再送したＢＵ（ＩＰパケット）に対するＢＡを一定期間後も受信しないことを検知すると、動的に更新される鍵の設定を初期化し、ＢＵを図５に示すように生成して（Ｓ５０１～Ｓ５０５）鍵送信装置（ＨＡ）１００に送信する（Ｓ５０６）。

【０２５２】

鍵送信装置（ＨＡ）１００は、図２２及び図２３に示すように、鍵受信装置（ＭＮ）からのＢＵが初期化鍵を用いて暗号化されたことを意味していると判定すると（Ｓ５０７～Ｓ５１４）、上記と同様に、鍵の生成等の処理を行い（Ｓ５１

５～Ｓ５１８）、ＢＡに最新の鍵を含んだ鍵配布メッセージを付加し（Ｓ５１９）、鍵受信装置（ＭＮ）に送信する（Ｓ５２０～Ｓ５２４）。

【０２５３】

図７、図１８に示すように、鍵受信装置（ＭＮ）は、鍵配布メッセージが付加されたＢＡを受信すると（Ｓ１２２）、その中に含まれる鍵を暗号化鍵(送信用)/復号化鍵(受信用)に設定する（Ｓ１２３～Ｓ１２９）。これについてはすでに述べたものと同様である。

【０２５４】

以上述べたように、本動作例によれば、鍵受信装置（ＭＮ）２００が鍵更新要求メッセージ又はそれに相当するメッセージを再送することにより、正常な状態（最新の鍵が鍵受信装置（ＭＮ）２００の送受信用に設定された状態）に復帰することが可能となる。また、鍵更新要求メッセージを再送してもその返答として鍵配布メッセージが鍵受信装置に届かない場合、鍵受信装置（ＭＮ）２００は鍵初期化要求メッセージを鍵送信装置（ＨＡ）１００に送信することによって、初期化を行う。

【０２５５】

以上述べたように、本動作例では、鍵受信側装置の障害等で鍵受信側装置と鍵送信側装置の動的鍵の不一致が起きた場合、動的鍵初期化メッセージ又はそれに相当するメッセージを鍵受信側装置が送信することにより、双方の動的鍵を初期化することが可能となる。

【０２５６】

次に変形例について説明する。

【０２５７】

上記２つの実施形態においては、鍵送信装置及び鍵受信装置間の通信は、Ｍｏｂｉｌｅ　ＩＰｖ６による通信であるように説明したが、本発明はこれに限定されない。鍵送信装置及び鍵受信装置間の通信として各種の通信を適用することが可能である。例えば、鍵送信装置及び鍵受信装置間の通信は、Ｍｏｂｉｌｅ　ＩＰｖ４による通信であってもよい。この場合、登録要求としてＩＰｖ６のＢＵに代えてRegistration Requestを、登録応答としてＩＰｖ６のＢＡに代えてRegist

ration Replyを、それぞれ用いる。これらは、例えば、ＩＰパケットのペイロード部分に設定（又は配置）される。

【０２５８】

また、上記２つの実施形態においては、鍵受信装置（ＭＮ）２００から鍵送信装置（ＨＡ）１００へはＢＵ及び所定メッセージ（又はＢＵのみ）が送信され、これに応じて、鍵送信装置（ＨＡ）１００が鍵配布メッセージを鍵受信装置（ＭＮ）２００に対して配布するように説明したが、本発明はこれに限定されない。例えば、鍵受信装置（ＭＮ）２００から鍵送信装置（ＨＡ）１００へは所定メッセージ（例えば鍵初期化要求メッセージ）のみを送信し、これに応じて、鍵送信装置（ＨＡ）１００が鍵配布メッセージを鍵受信装置（ＭＮ）２００に対して配布するようにしてもよい。

【０２５９】

また、上記２つの実施形態においては、鍵送信装置（ＨＡ）１００と鍵受信装置（ＭＮ）２００とがそれぞれ、共通の鍵であって世代の異なる鍵を送信用の鍵として設定するように説明したが、本発明はこれに限定されない。例えば、鍵送信装置（ＨＡ）１００に送信用鍵としてＮ－１世代のＡ鍵を、鍵受信装置（ＭＮ）２００に送信用鍵としてＮ世代のＢ鍵を、それぞれ設定する。そして、鍵送信装置（ＨＡ）１００に受信用鍵としてＮ世代及びＮ－１世代のＢ鍵を、そして、鍵受信装置（ＭＮ）２００に受信用としてＮ世代及びＮ－１世代のＡ鍵を、それぞれ設定するようにしてもよい。

【０２６０】

また、上記２つの実施形態においては、鍵送信装置がＭｏｂｉｌｅ　ＩＰにおけるＨＡであり、鍵受信装置がＭｏｂｉｌｅ　ＩＰにおけるＭＮであるように説明したが、本発明はこれに限定されない。例えば、鍵送信装置がインターネット上のサーバ装置であり、鍵受信装置がそのサーバと通信を行うクライアント装置であってもよい。

【０２６１】

なお、上記２つの実施形態においては、ＢＵ及びＢＡがＩＰｖ６の拡張ヘッダ部分（又はペイロード部分）に設定（又は配置）されるように説明したが、本発

明はこれに限定されない。ＩＰｖ６の仕様については、現状ドラフトの段階である。例えば、ドラフト15版(draft-ietf-mobileip-ipv6-15.txt)においては、ＢＵ/ＢＡ共 終点オプション(destination option)に含まれる。また、ドラフト18版(draft-ietf-mobileip-ipv6-18.txt)においては、ＢＵ/ＢＡ共 モビリティヘッダ(mobility header)に含まれる。従って、ＢＵ、ＢＡの設定（配置）は、仕様の変化に応じて適宜に改良することが可能である。

【０２６２】

［その他］　本発明は、以下のように特定することができる。

（付記１）　鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第１保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第１設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第２保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第２設定手段と、を備える、共通鍵暗号化通信システム。（１）

（付記２）　前記鍵送信装置は、暗号化鍵を取得する取得手段をさらに備え、前記第１保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第１設定手段は、前記第１保持手段による更新後の保持鍵に基づいて、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、付記１に記載の共通鍵暗号化通信システム。（２）

（付記３）　前記鍵送信装置は、暗号化鍵を生成する生成手段を備え、前記取得手段は、前記生成手段によって生成された暗号化鍵を取得する、付記２に記載の共通鍵暗号化通信システム。（３）

（付記４）　前記鍵送信装置は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する第１送信手段をさらに備える、付記２に記載の共通鍵暗

号化通信システム。（４）

（付記５）　前記鍵受信装置は、前記鍵送信装置から送信される暗号化鍵を受信する第２受信手段をさらに備え、前記第２受信手段が暗号化鍵を受信した場合、前記第２保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記第２受信手段によって受信した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持し、前記第２設定手段は、前記第２保持手段による更新号の保持鍵に基づいて、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ再設定する、付記４に記載の共通鍵暗号化通信システム。（５）

（付記６）　前記鍵受信装置は、所定メッセージを鍵送信装置に対して送信する第２送信手段を備え、前記鍵送信装置は、前記鍵受信装置から送信される所定メッセージを受信する第１受信手段を備える、付記１に記載の共通鍵暗号化システム。（６）

（付記７）　前記第１及び第２保持手段は、それぞれ初期化鍵を保持する、付記４に記載の共通鍵暗号化通信システム。（７）

（付記８）　前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵初期化要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵初期化要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第１保持手段は、共通の初期化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する、付記７に記載の共通鍵暗号化通信システム。

（付記９）　前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵更新要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵更新要求メッセージを受信した場合、前記取得手段は、暗号化鍵を取得し、前記第１保持手段は、前記最新の暗号化鍵を一世代前の暗号化鍵として、前記取得手段によって取得した暗号化鍵を最新の暗号化鍵として、それぞれ更新して保持する、付記４に記載の共通鍵暗号化通信システム。

（付記１０）　前記鍵受信装置は、鍵更新時期を決定するための手段を備え、前記第２送信手段は、鍵更新時期に達した場合に、鍵更新要求メッセージを鍵送信

装置に対して送信する、付記９に記載の共通鍵暗号化通信システム。

（付記１１）　前記鍵送信装置は、鍵更新時期を決定するための手段を備え、第１送信手段は、鍵更新時期に達した場合に、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、付記４に記載の共通鍵暗号化通信システム。

（付記１２）　前記鍵受信装置は、所定タイミングで前記所定メッセージとして鍵再送要求メッセージを鍵送信装置に対して送信し、前記鍵送信装置が前記鍵受信装置から送信される鍵再送要求メッセージを受信した場合、第１送信手段は、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、付記４に記載の共通鍵暗号化通信システム。

（付記１３）　前記第１送信手段は、前記第１及び第２保持手段がいずれの鍵も保持していない状態で、前記取得手段によって取得した暗号化鍵を鍵受信装置に対して送信する、請求項４に記載の共通鍵暗号化通信システム。

（付記１４）　鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵送信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵送信装置。（８）

（付記１５）　鍵送信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う鍵受信装置であって、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する設定手段とを備える、鍵受信装置。（９）

（付記１６）　鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行う方法であって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定し、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持し、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵

及び一世代前の暗号化鍵を、それぞれ設定する、共通鍵暗号化通信方法。（１０）

【０２６３】

本発明は、その精神または主要な特徴から逸脱することなく、他の様々な形で実施することができる。このため、上記の実施形態はあらゆる点で単なる例示にすぎず、これらの記載によって本発明が限定的に解釈されるものではない。

【０２６４】

【発明の効果】

以上説明したように、本発明によれば、共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も暗号化通信を継続することが可能となる。また、一対多の暗号化通信（例えばMobile IPにおけるＭＮとＨＡ間や、インターネット上のサーバとそれに接続するクライアント間等の通信）を行う場合に、ＨＡやインターネット上のサーバの負荷の低減が可能となる。またセキュリティを高めるための動的な鍵更新を行った場合も、それに伴って通信断が発生しない。

【図面の簡単な説明】

【図１】

本発明の実施の形態である共通鍵暗号化通信システムの概略構成を説明するための図である。

【図２】

鍵送信装置（ＨＡ）の構成例を説明するための図である。

【図３】

鍵受信装置（ＭＮ）の構成例を説明するための図である。

【図４】

鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図５】

鍵受信装置（ＭＮ）に着目したシーケンス図である。

【図６】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図７】

鍵受信装置（ＭＮ）に着目したシーケンス図である。

【図８】

鍵受信装置（ＭＮ）からの鍵更新要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図９】

鍵受信装置（ＭＮ）に着目したシーケンス図である。

【図１０】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図１１】

鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図１２】

鍵受信装置（ＭＮ）に着目したシーケンス図である。

【図１３】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図１４】

鍵送信側装置(ＨＡ)が鍵の更新を判断して、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図１５】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図１６】

鍵送信装置（ＨＡ）のみ鍵が更新された状態を説明するための図である。

【図１７】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【図１８】

鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである

。

【図１９】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【図２０】

鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャートである。

【図２１】

鍵－ＳＰＩ対応テーブルの例を説明するための図である。

【図２２】

鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図２３】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図２４】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図２５】

鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図である。

【図２６】

鍵受信装置（ＭＮ）に着目したシーケンス図である。

【図２７】

鍵送信装置（ＨＡ）に着目したシーケンス図である。

【図２８】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャートである。

【符号の説明】

１００　　鍵送信装置

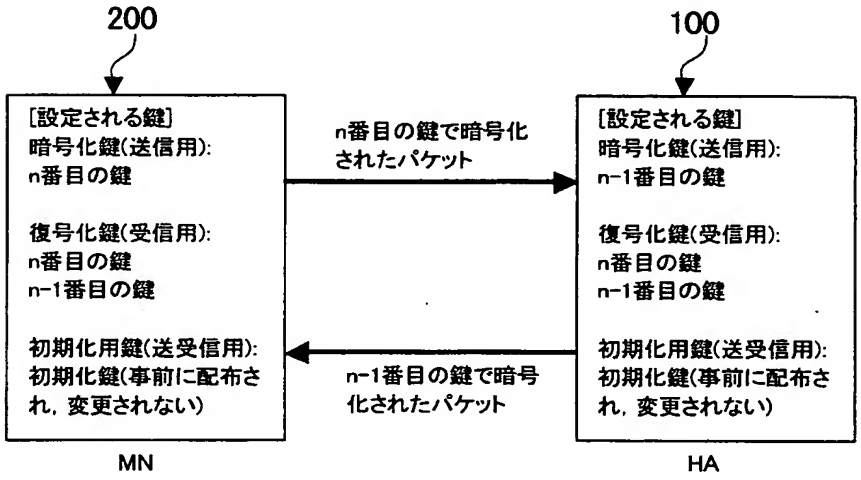
１０１　　パケット送受信部

１０２　　鍵生成／管理部
１０３　　暗号化／復号化部
１０４　　プロトコル制御部
２００　　鍵受信装置
２０１　　パケット送受信部
２０２　　鍵管理部
２０３　　暗号化／復号化部
２０４　　プロトコル制御部

【書類名】　図面

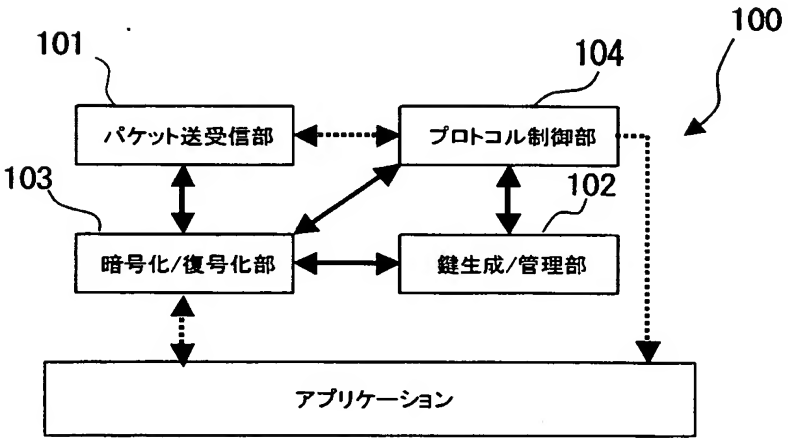
【図１】

本発明の実施の形態である共通鍵暗号化通信システムの概略構成を説明するための図
（動的鍵を用いた暗号化通信（定常状態））



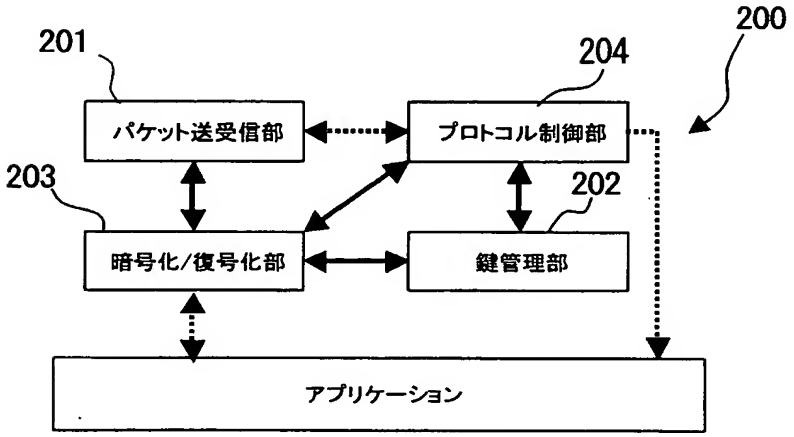
【図２】

鍵送信装置（ＨＡ）の構成例を説明するための図である(鍵送信側装置(HA)の構成例)



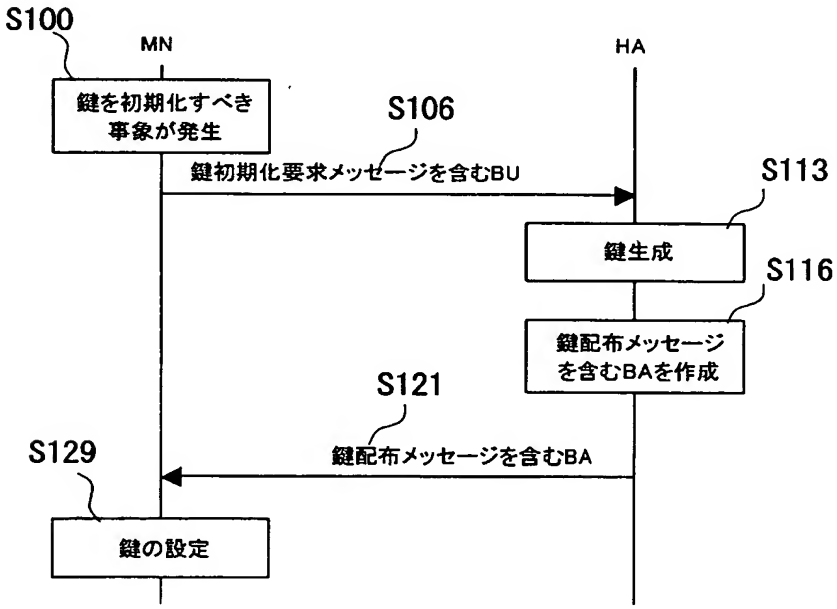
【図３】

鍵受信装置（MN）の構成例を説明するための図である（鍵受信側装置（MN）の構成例）



【図４】

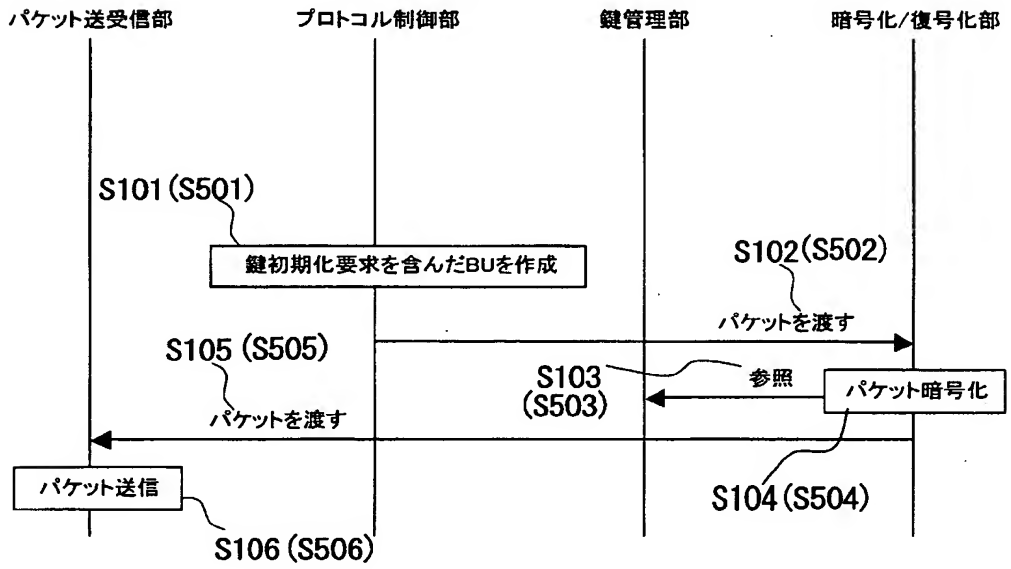
鍵受信装置（MN）起動時に動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図
（鍵初期化シーケンス（鍵初期化要求メッセージを用いる場合））



【図５】

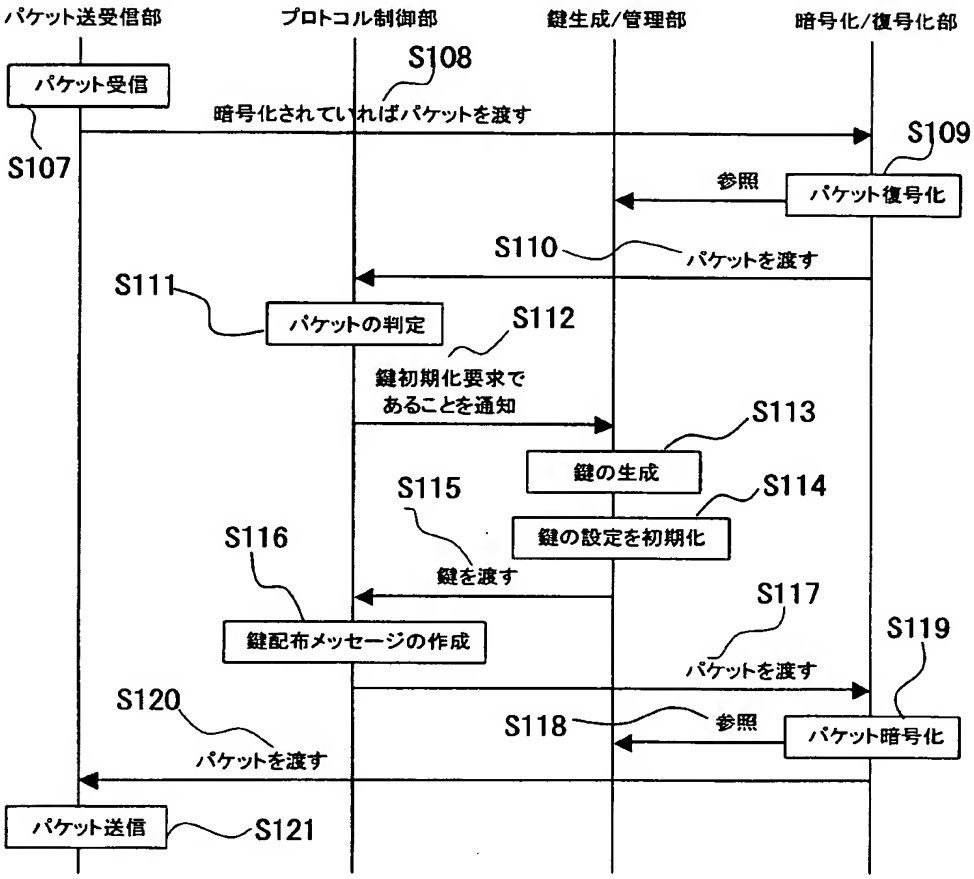
鍵受信装置（MN）に着目したシーケンス図

（MNが鍵の更新を判断する場合のシーケンス（鍵初期化メッセージを用いる場合））



【図６】

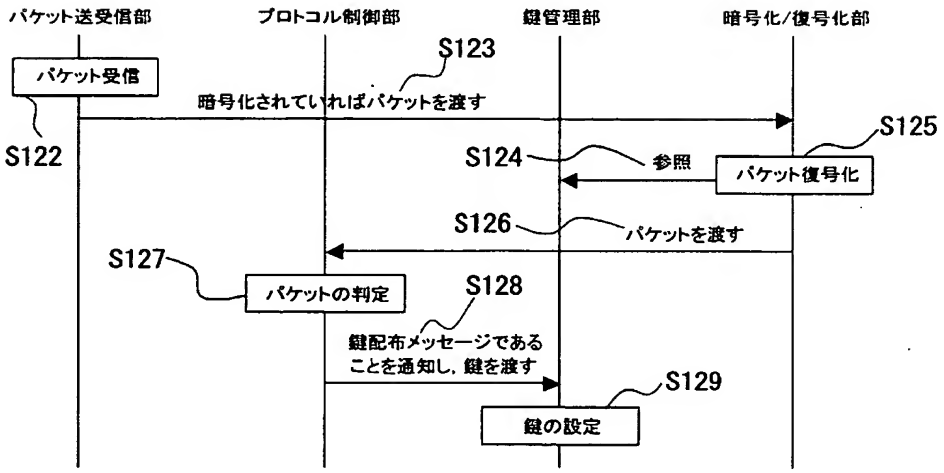
鍵送信装置（ＨＡ）に着目したシーケンス図
(HAが鍵初期化要求メッセージを受信した場合のシーケンス)



【図７】

鍵受信装置（MN）に着目したシーケンス図

（鍵配布メッセージ受信時のMNのシーケンス）



【図８】

鍵受信装置（ＭＮ）からの鍵更新要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図(MNが鍵更新の契機を判断する場合の鍵配布シーケンス(鍵更新要求メッセージを用いる場合))

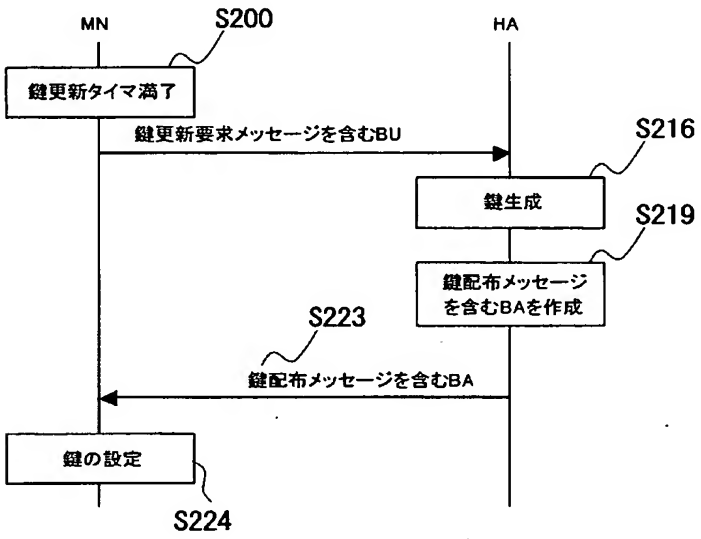
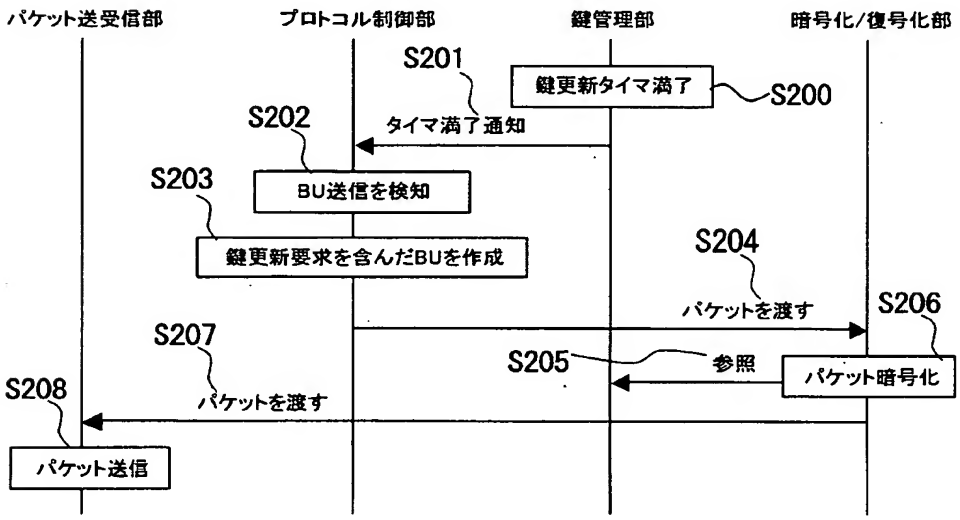


図 1:

【図９】

鍵受信装置（ＭＮ）に着目したシーケンス図

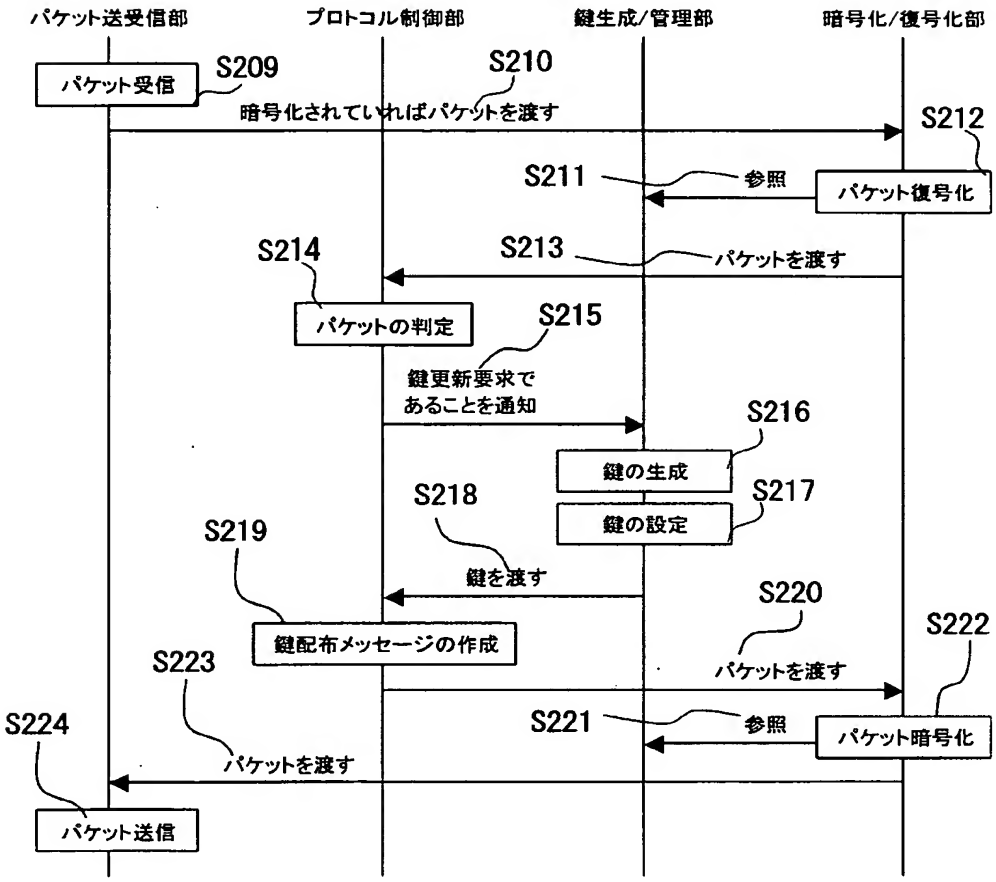
（MNが鍵の更新を判断する場合のシーケンス（鍵更新メッセージを用いる場合））



【図１０】

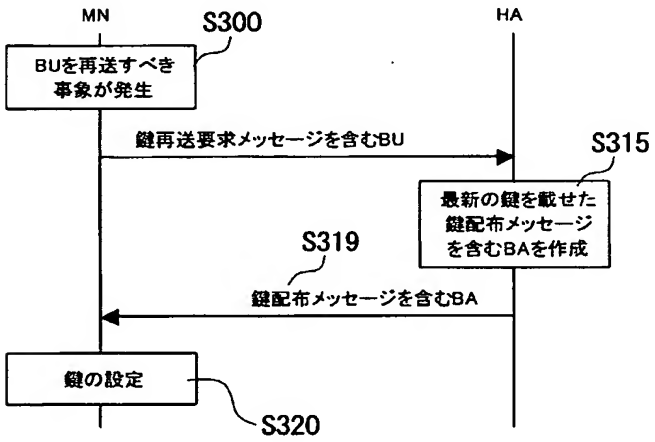
鍵送信装置（ＨＡ）に着目したシーケンス図

(HAが鍵更新要求メッセージを受信した場合のシーケンス)



【図１１】

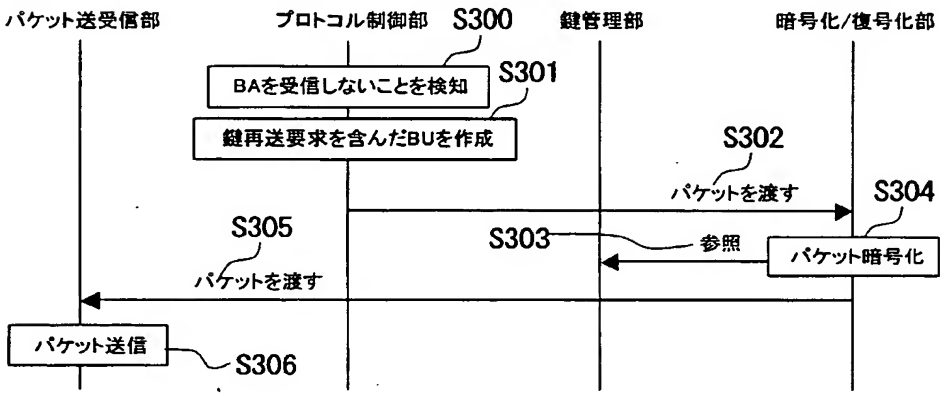
鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図(BU再送時の鍵配布シーケンス(再送前のBUが鍵更新/鍵再送要求メッセージだった場合))



【図１２】

鍵受信装置（MN）に着目したシーケンス図

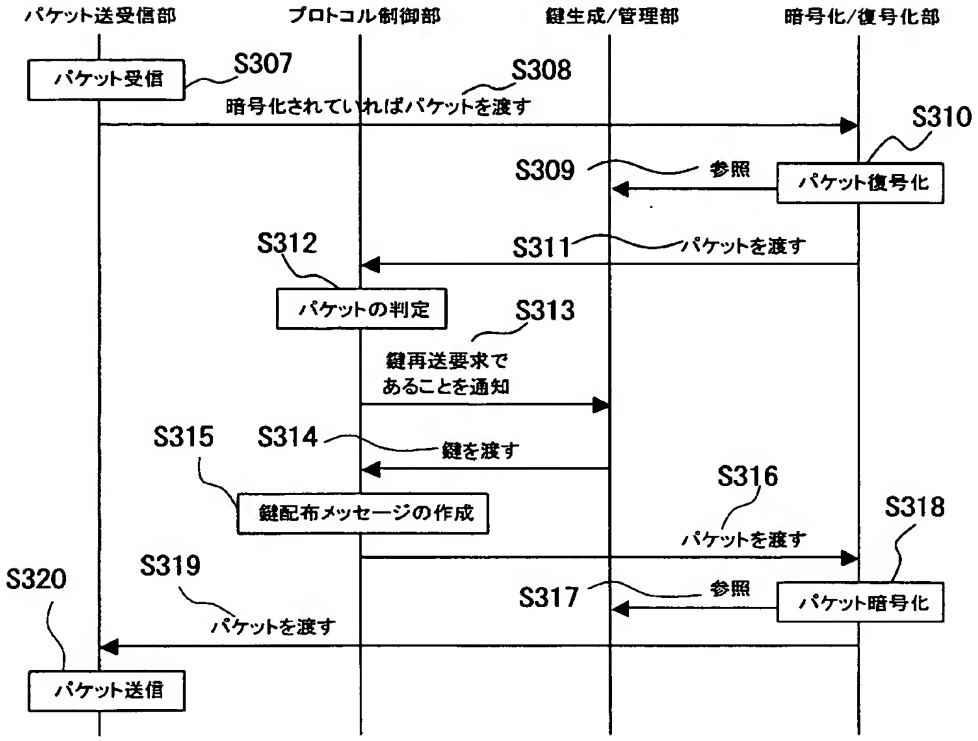
（鍵配布メッセージが破棄された場合にMNのシーケンス（鍵再送メッセージを用いる場合））



【図１３】

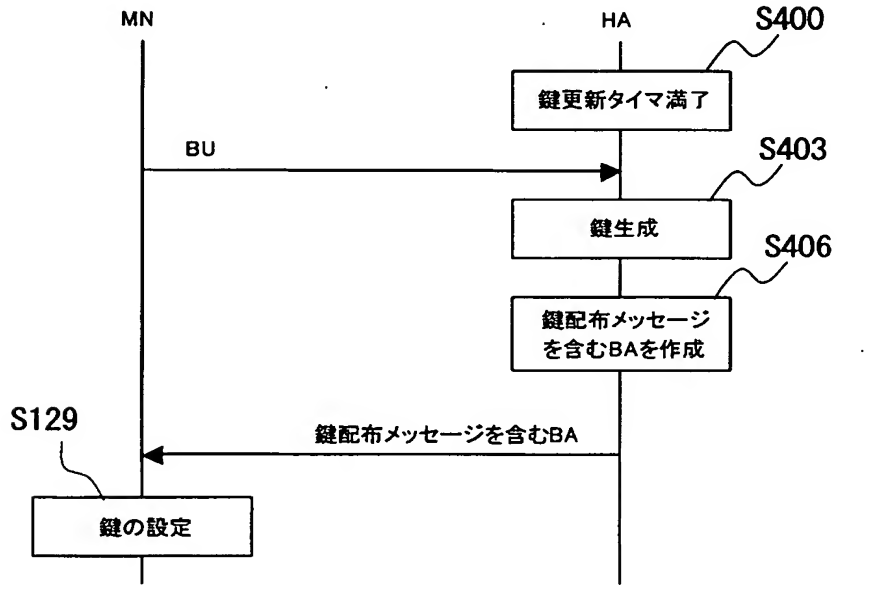
鍵送信装置（ＨＡ）に着目したシーケンス図

（ HA が鍵再送要求メッセージを受信した場合のシーケンス）



【図１４】

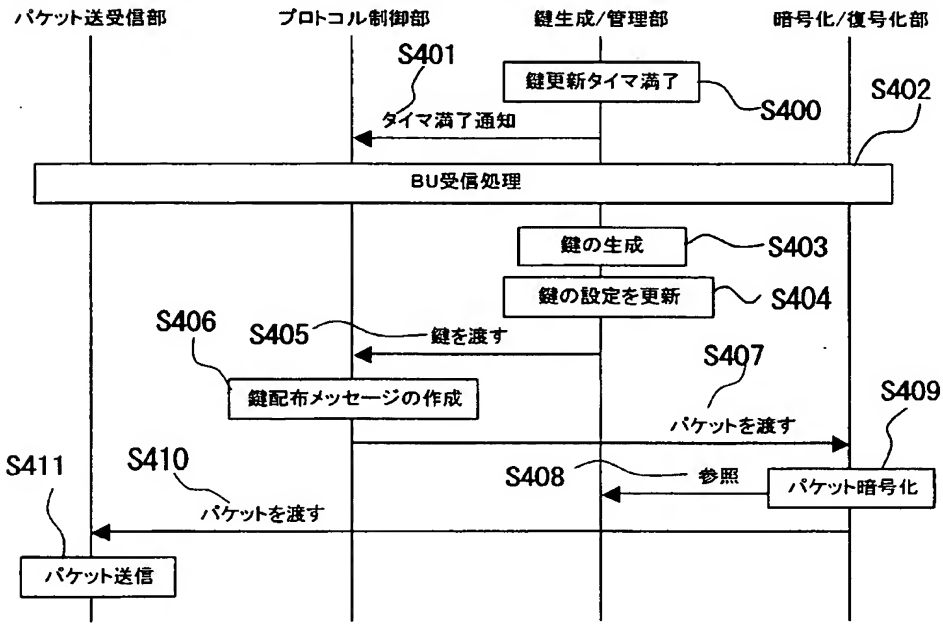
鍵送信側装置（ＨＡ）が鍵の更新を判断して、動的鍵（共通鍵）を配布する手順を説明するためのシーケンス図（HAが鍵更新の契機を判断する場合の鍵配布シーケンス）



【図１５】

鍵送信装置（ＨＡ）に着目したシーケンス図

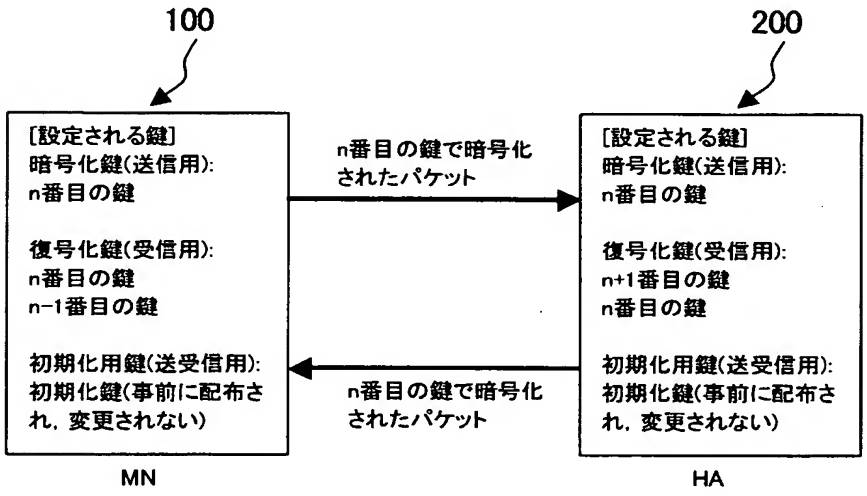
(HAが鍵の更新を判断する場合のシーケンス(鍵更新/初期化/再送メッセージを用いる場合))



【図１６】

鍵送信装置（ＨＡ）のみ鍵が更新された状態を説明するための図

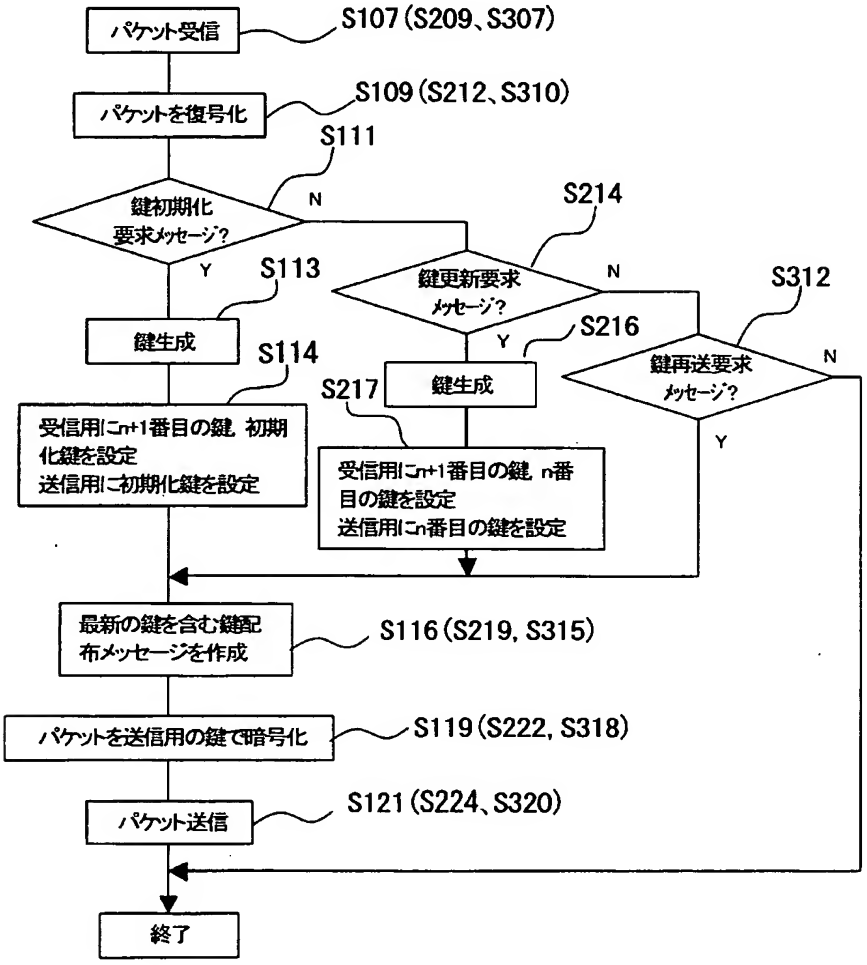
（ 動的鍵を用いた暗号化通信(HA のみ鍵が更新された状態)）



【図１７】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャート

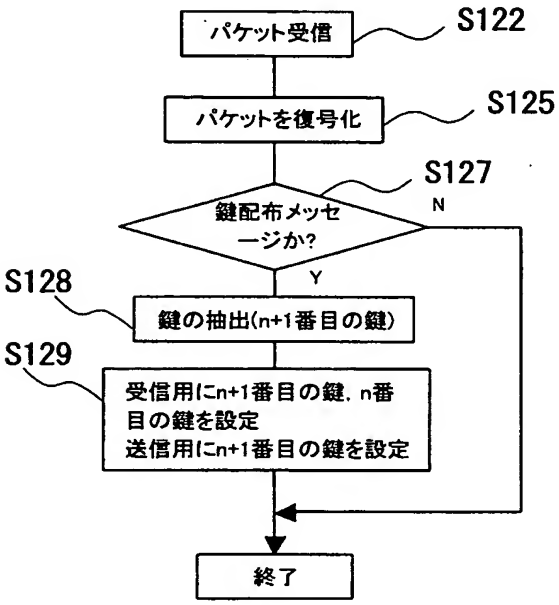
（パケット受信時の鍵送信側装置(HA)での処理フロー(鍵初期化/更新/再送要求メッセージを用いる場合)）



【図１８】

鍵受信装置（MN）における概略処理を説明するためのフローチャート

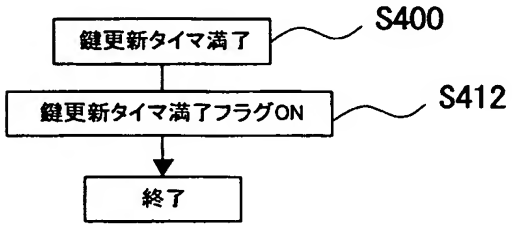
（パケット受信時の鍵受信側装置(MN)での処理フロー）



【図１９】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャート

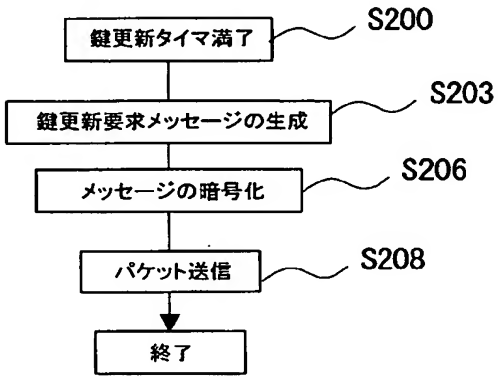
（ HA が持つ鍵更新タイマ満了時の処理フロー(HA が鍵の更新を判断する場合)）



【図２０】

鍵受信装置（ＭＮ）における概略処理を説明するためのフローチャート

（ＭＮが持つ鍵更新タイマ満了時の処理フロー（ＭＮが鍵の更新を判断し，鍵更新要求メッセージを用いる場合））



【図２１】

鍵－ＳＰＩ対応テーブルの例を説明するための図

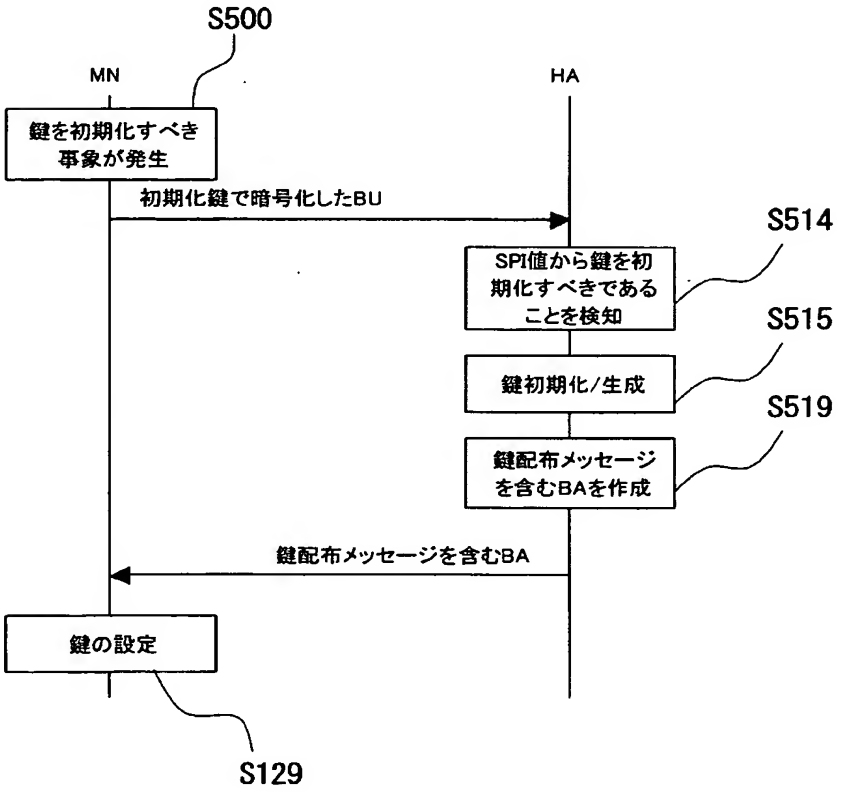
（鍵-SPI 対応テーブル）

鍵	SPI
初期化鍵	1001
n-1 番目の鍵	2001
n 番目の鍵	2002

【図２２】

鍵受信装置（ＭＮ）起動時に動的鍵（共通鍵）を配布する手順を説明するための

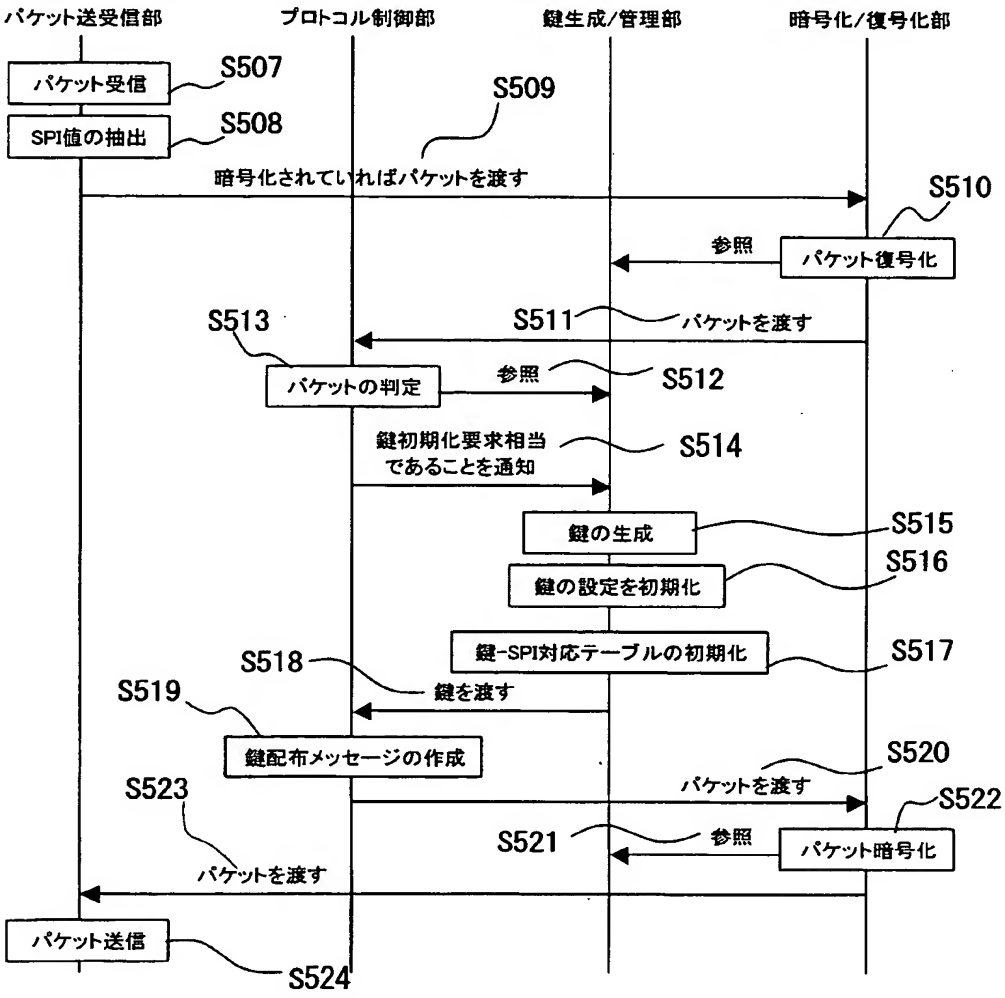
シーケンス図（鍵初期化シーケンス（SPI 値で鍵初期化を判断する場合））



【図２３】

鍵送信装置（ＨＡ）に着目したシーケンス図

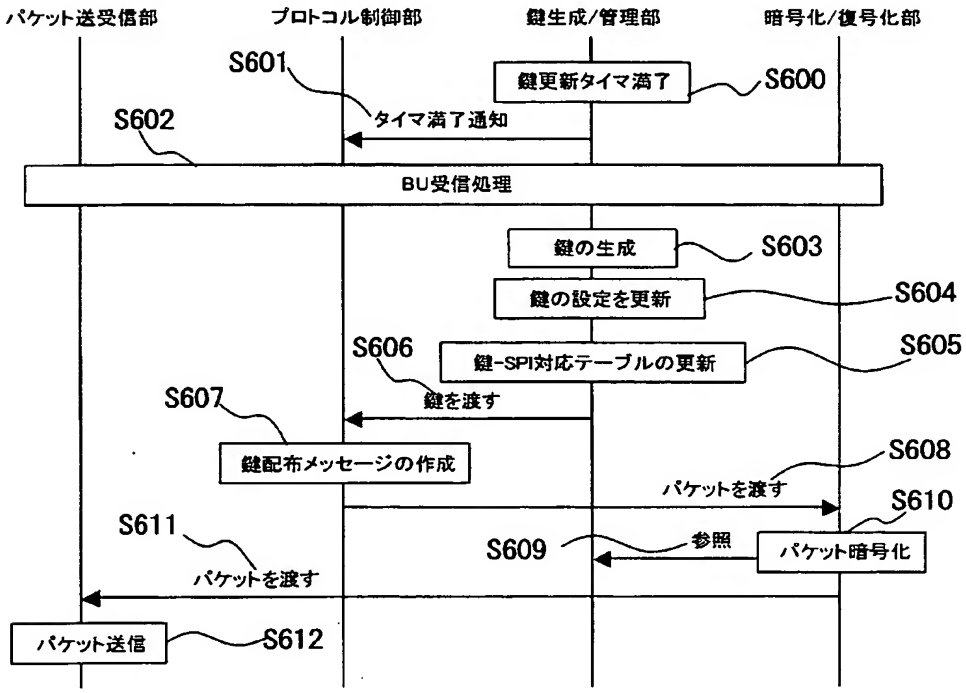
(HAが鍵初期化要求メッセージ相当のBUを受信した場合のシーケンス)



【図２４】

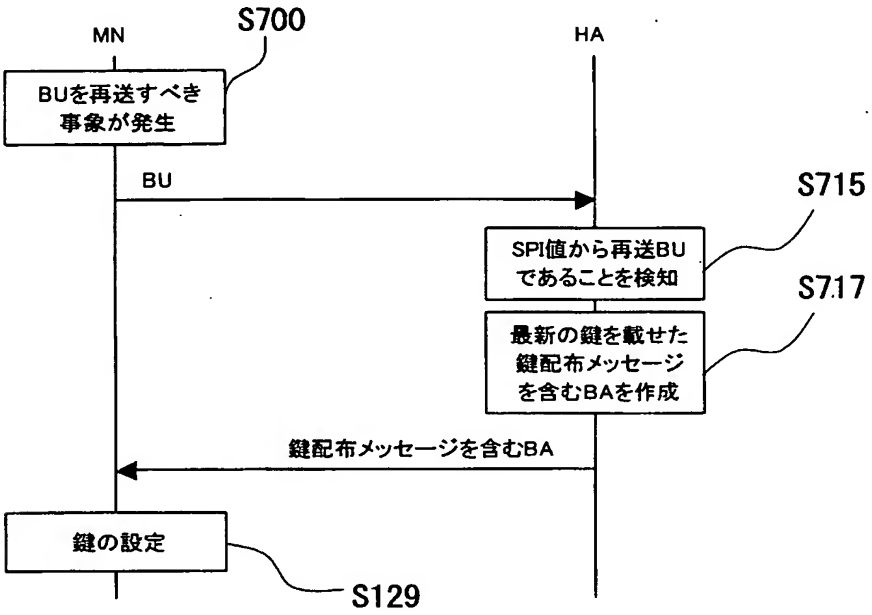
鍵送信装置（ＨＡ）に着目したシーケンス図

（ HA が鍵の更新を判断する場合のシーケンス(SPI 値を用いる場合)）



【図２５】

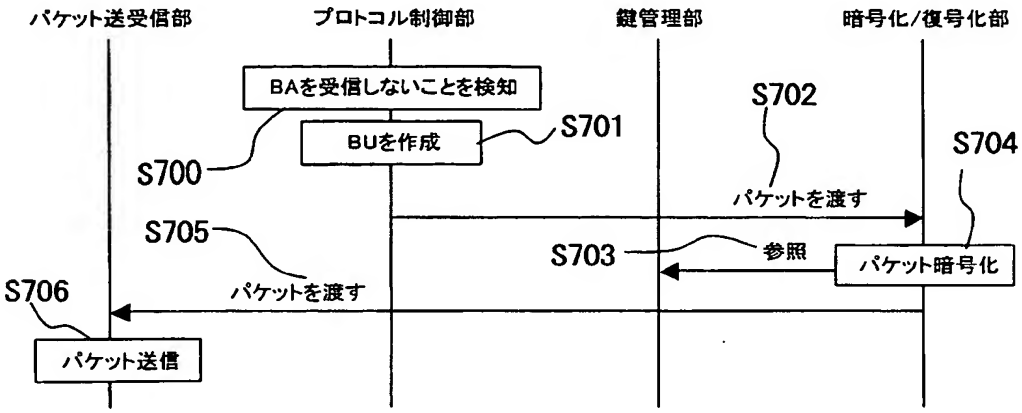
鍵受信装置（ＭＮ）からの鍵再送要求メッセージにより、動的鍵（共通鍵）を配する手順を説明するためのシーケンス図（ BU 再送時の鍵配布シーケンス（SPI 値を用いて再送 BU を判断する場合））



【図２６】

鍵受信装置（MN）に着目したシーケンス図

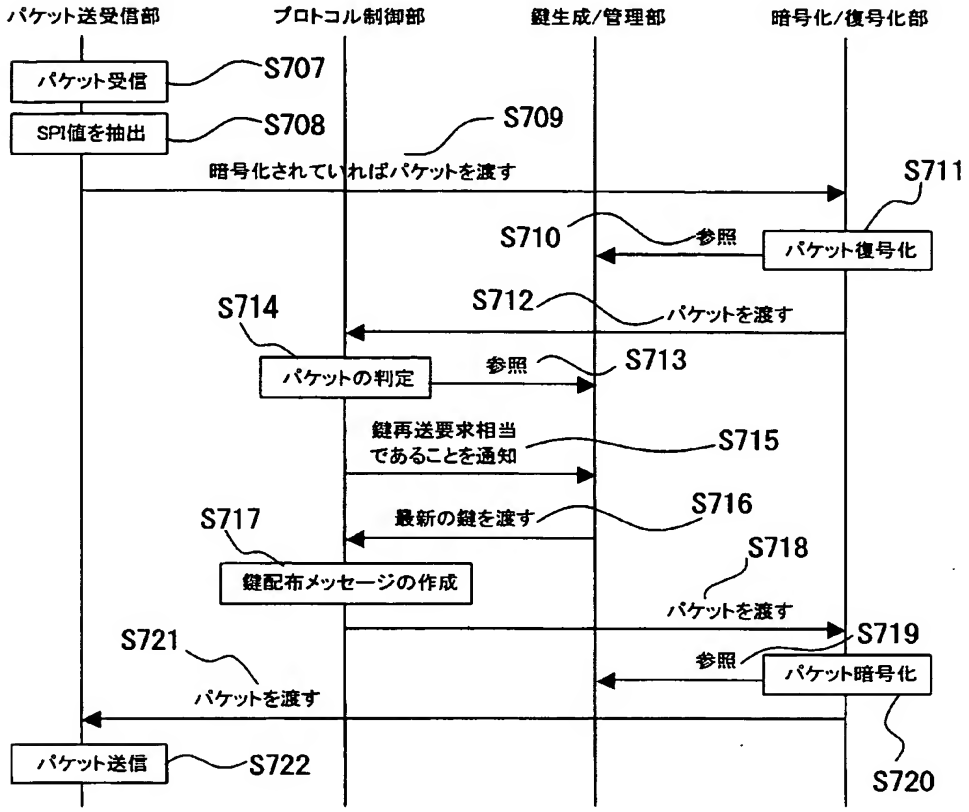
（鍵配布メッセージが破棄された場合のMNのシーケンス(SPI値を用いる場合)）



【図２７】

鍵送信装置（ＨＡ）に着目したシーケンス図

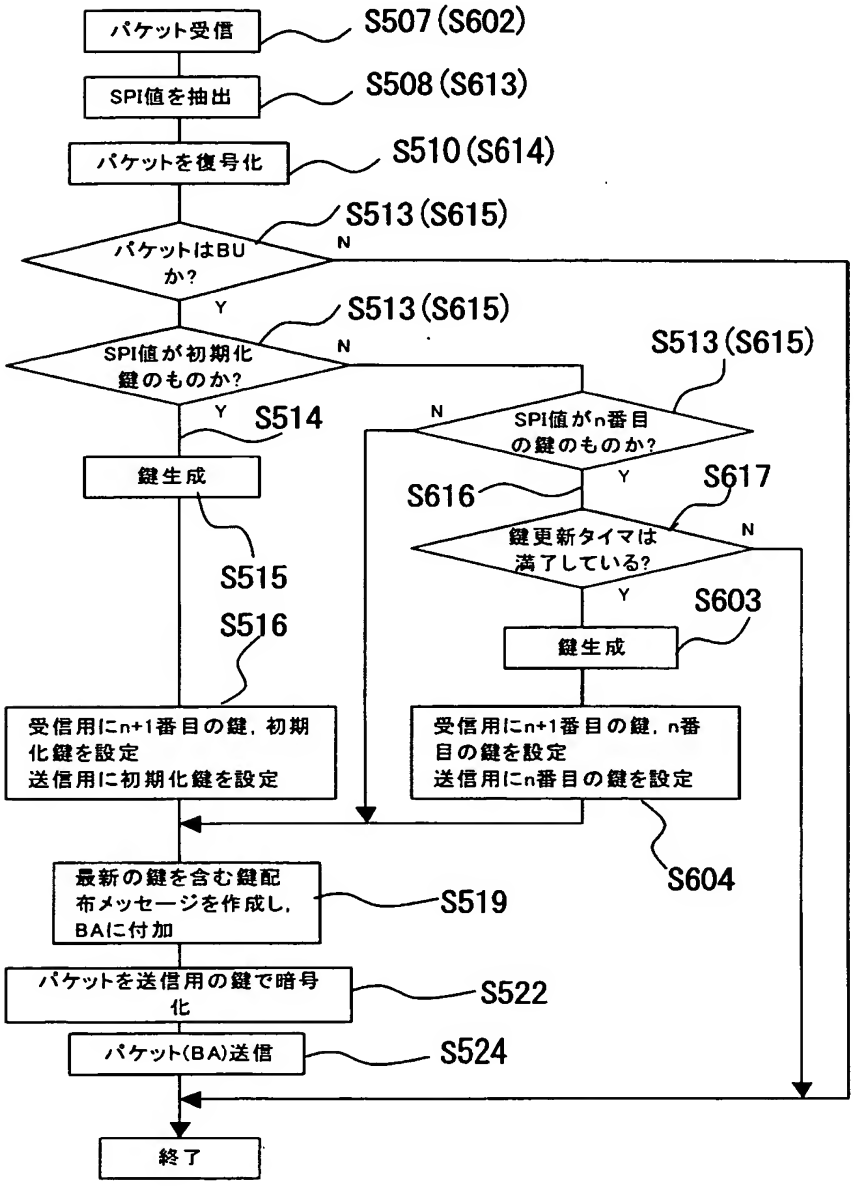
（HAが鍵再送要求メッセージ相当のBUを受信した場合のシーケンス））



【図２８】

鍵送信装置（ＨＡ）における概略処理を説明するためのフローチャート

（パケット受信時の鍵送信側装置(HA)での処理フロー(SPI 値を用いる場合)）



【書類名】　要約書

【要約】

【課題】　共通鍵暗号化通信を行う二つの装置の一方が他方に暗号化鍵を配布する場合、配布手順の最中及び暗号化鍵（鍵配布メッセージ）が破棄された場合も通信を継続する。

【解決手段】　鍵送信装置と鍵受信装置との間で、所定タイミングで更新される共通鍵による暗号化通信を行うシステムであって、前記鍵送信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第１保持手段と、送信用として一世代前の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第１設定手段と、を備え、前記鍵受信装置は、前記共通鍵として最新の暗号化鍵及び一世代前の暗号化鍵を保持する第２保持手段と、送信用として最新の暗号化鍵を、受信用として最新の暗号化鍵及び一世代前の暗号化鍵を、それぞれ設定する第２設定手段と、を備える。

【選択図】　図１

特願２００２－３４８７４８

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　　神奈川県川崎市中原区上小田中１０１５番地
氏　名　　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社